Extreme Networks EAS 200-24p Switch Software Manual

Layer 2 Managed PoE Ethernet Switch

Release 1.00

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: July 2011
Part number: 120708-00 Rev. 01

AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2011 Extreme Networks, Inc. All Rights Reserved.

Table of Contents

Preface Template Formats 9

Intended Readers 9
Typographical Conventions 9
Notes, Cautions, and Warnings 9

Chapter 1: Web-based Switch Configuration 11

Introduction 11
Login to the Web Manager 11
Web-based User Interface 12
Areas of the User Interface 13
Web Pages 13

Chapter 2: System Configuration 15

Device Information 15
System Information Settings 16
Port Configuration 16
Port Settings 16
Port Description Settings 18
Port Error Disabled 19
Jumbo Frame Settings 20
PoE 20
PoE System Settings 22
PoE Port Settings 23
Serial Port Settings 24
Warning Temperature Settings 25
System Log configuration 26
System Log Settings 26
System Log Server Settings 26
System Log 27
System Log & Trap Settings 28
System Severity Settings 29
Time Range Settings 30
Port Group Settings 31
Time Settings 32
User Accounts Settings 32
Command Logging Settings 33

Chapter 3: Management 35

ARP 35
Static ARP Settings 35
Proxy ARP Settings 36
ARP Table 36
Gratuitous ARP 37
Gratuitous ARP Global Settings 37
Gratuitous ARP Settings 38
IPv6 Neighbor Settings 39
IP Interface 41

System IP Address Settings....41
Interface Settings....42
Management Settings....45
Session Table....47
SNMP Settings....47
SNMP Global Settings....48
SNMP Traps Settings....49
SNMP Linkchange Traps Settings....49
SNMP View Table Settings....50
SNMP Community Table Settings....51
SNMP Group Table Settings....52
SNMP Engine ID Settings....54
SNMP User Table Settings....54
SNMP Host Table Settings....55
SNMPv6 Host Table Settings....56
RMON Settings....57
Telnet Settings....58
Web Settings....59

Chapter 4: L2 Features....61

VLAN....61
802.1Q VLAN Settings....67
802.1v Protocol VLAN....70
802.1v Protocol Group Settings....70
802.1v Protocol VLAN Settings....72
Asymmetric VLAN Settings....73
GVRP....73
GVRP Global Settings....73
GVRP Port Settings....74
MAC-based VLAN Settings....75
Private VLAN Settings....76
PVID Auto Assign Settings....78
Voice VLAN....79
Voice VLAN Global Settings....79
Voice VLAN Port Settings....80
Voice VLAN OUI Settings....80
Voice VLAN Device....81
VLAN Trunk Settings....82
Browse VLAN....83
Show VLAN Ports....83
QinQ....84
QinQ Settings....86
VLAN Translation Settings....87
Spanning Tree....88
STP Bridge Global Settings....90
STP Port Settings....91
MST Configuration Identification....93
STP Instance Settings....94
MSTP Port Information....95
Link Aggregation....96
Port Trunking Settings....97
LACP Port Settings....98
FDB....99
Static FDB Settings....99
Unicast Static FDB Settings....99
Multicast Static FDB Settings....100
MAC Notification Settings....101

MAC Address Aging Time Settings 102
MAC Address Table 103
ARP & FDB Table 104
L2 Multicast Control 105
IGMP Snooping 105
IGMP Snooping Settings 105
IGMP Snooping Rate Limit Settings 108
IGMP Snooping Static Group Settings 109
IGMP Router Port 110
IGMP Snooping Group 111
IGMP Snooping Forwarding Table 112
IGMP Snooping Counter 112
MLD Snooping 113
MLD Snooping Settings 115
MLD Snooping Rate Limit Settings 118
MLD Snooping Static Group Settings 118
MLD Router Port 120
MLD Snooping Group 120
MLD Snooping Forwarding Table 121
MLD Snooping Counter 122
Multicast Filtering 123
IPv4 Multicast Filtering 123
IPv4 Multicast Profile Settings 123
IPv4 Limited Multicast Range Settings 125
IPv4 Max Multicast Group Settings 126
IPv6 Multicast Filtering 127
IPv6 Multicast Profile Settings 127
IPv6 Limited Multicast Range Settings 128
IPv6 Max Multicast Group Settings 129
Multicast Filtering Mode 130
LLDP 131
LLDP Global Settings 131
LLDP Port Settings 133
LLDP Management Address List 134
LLDP Basic TLVs Settings 134
LLDP Dot1 TLVs Settings 135
LLDP Dot3 TLVs Settings 136
LLDP Statistic System 137
LLDP Local Port Information 138
LLDP Remote Port Information 139
NLB FDB Settings 140

Chapter 5: L3 Features 143

IPv4 Static/Default Route Settings 143
IPv4 Route Table 144
IPv6 Static/Default Route Settings 144
IP Forwarding Table 146

Chapter 6: QoS 147

802.1p Settings 149
802.1p Default Priority Settings 149
802.1p User Priority Settings 150
Bandwidth Control 150
Bandwidth Control Settings 150
Queue Bandwidth Control Settings 152
Traffic Control Settings 153
DSCP 154

DSCP Trust Settings 154
DSCP Map Settings 155
HOL Blocking Prevention 156
Scheduling Settings 157
QoS Scheduling 157
QoS Scheduling Mechanism 158

Chapter 7: ACL 161

ACL Configuration Wizard 161
Access Profile List 162
Add an Ethernet ACL Profile 163
Adding an IPv4 ACL Profile 168
Adding an IPv6 ACL Profile 173
Adding a Packet Content ACL Profile 178
ACL Finder 183
ACL Flow Meter 183
Egress Access Profile List 188
Add an Ethernet ACL Profile 189
Adding an IPv4 ACL Profile 193
Adding an IPv6 ACL Profile 198
Egress ACL Flow Meter 202

Chapter 8: Security 207

802.1X 207
802.1X Global Settings 211
802.1X Port Settings 212
802.1X User Settings 213
Guest VLAN Settings 214
RADIUS 216
Authentication RADIUS Server Settings 216
RADIUS Accounting Settings 217
RADIUS Authentication 218
RADIUS Account Client 220
MAC-based Access Control (MAC) 221
MAC-based Access Control Settings 222
MAC-based Access Control Local Settings 223
MAC-based Access Control Authentication State 225
Web-based Access Control (WAC) 225
WAC Global Settings 227
WAC User Settings 228
WAC Port Settings 229
WAC Authentication State 230
Compound Authentication 231
Compound Authentication Settings 231
Port Security 232
Port Security Settings 232
Port Security VLAN Settings 234
Port Security Entries 235
BPDU Attack Protection 235
Loopback Detection Settings 237
Traffic Segmentation Settings 238
Access Authentication Control 238
Enable Admin 240
Authentication Policy Settings 241
Application Authentication Settings 242
Authentication Server Group Settings 243

Authentication Server Settings 244
Login Method Lists Settings 246
Enable Method Lists Settings 247
Local Enable Password Settings 249
SSL Settings 249
SSH 252
SSH Settings 253
SSH Authentication Method and Algorithm Settings 254
SSH User Authentication List 256
Trusted Host Settings 257

Chapter 9: Network Application 259

DHCP 259
DHCP Relay 259
DHCP Relay Global Settings 259
DHCP Relay VLAN Settings 262
DHCP Local Relay Settings 262
SNTP 263
SNTP Settings 263
Time Zone Settings 264
Flash File System Settings 265

Chapter 10: OAM 269

CFM 269
CFM Settings 269
CFM Port Settings 277
CFM MIPCCM Table 278
CFM Loopback Settings 278
CFM Linktrace Settings 279
CFM Packet Counter 280
CFM Fault Table 281
CFM MP Table 281
Ethernet OAM 282
Ethernet OAM Settings 282
Ethernet OAM Configuration Settings 283
Ethernet OAM Event Log 284
Ethernet OAM Statistics 284
Cable Diagnostics 285

Chapter 11: Monitoring 287

Utilization 287
CPU Utilization 287
DRAM & Flash Utilization 288
Port Utilization 288
Statistics 290
Port Statistics 290
Packets 290
Received (RX) 290
UMB_Cast (RX) 292
Transmitted (TX) 294
Errors 296
Received (RX) 296
Transmitted (TX) 298
Packet Size 300
Mirror 302
Port Mirror Settings 302

RSPAN Settings 303
sFlow 304
sFlow Global Settings 305
sFlow Analyzer Server Settings 305
sFlow Flow Sampler Settings 307
sFlow Counter Poller Settings 308
Ping Test 308
Trace Route 310
Peripheral 311
Device Environment 311

Chapter 12: Save and Tools 313

Save Configuration / Log 313
Download firmware 314
Download Firmware From TFTP 314
Download Firmware From HTTP 315
Upload Firmware 315
Upload Firmware To TFTP 315
Download Configuration 316
Download Configuration From TFTP 316
Download Configuration From HTTP 317
Upload Configuration 317
Upload Configuration To TFTP 317
Upload Configuration To HTTP 318
Upload Log File 318
Upload Log To TFTP 319
Upload Log To HTTP 319
Reset 320
Reboot System 321

Appendix A: System Log Entries 323

Appendix B: Trap Log Entries 337

Preface Template Formats

Intended Readers

The *EAS 200-24p Software Manual* contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Click on the **Apply** button. Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: **You have mail**. **Bold** font is also used to represent filenames, program names and commands. For example: **use the copy command**.
`Boldface Typewriter Font`	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Cautions, and Warnings

NOTE

A NOTE indicates important information that helps make better use of the device.

CAUTION

A CAUTION indicates either potential damage to hardware or loss of data and tells how to avoid the problem.

WARNING!

A WARNING indicates a potential for property damage, personal injury, or death.

CHAPTER 1

Web-based Switch Configuration

Introduction

All software functions of the **EAS 200-24p** switch can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard browser. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Login to the Web Manager

To begin managing the Switch, simply run the browser installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://192.168.69.123, where the numbers represent the IP address of the Switch.

This opens the management module's user authentication window, as seen below.

Figure 1: Enter Network Password window

Windows Security
The server 192.168.69.123 at Welcome requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin
Password
Remember my credentials
OK
Cancel

Enter the **Username** and **Password** and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

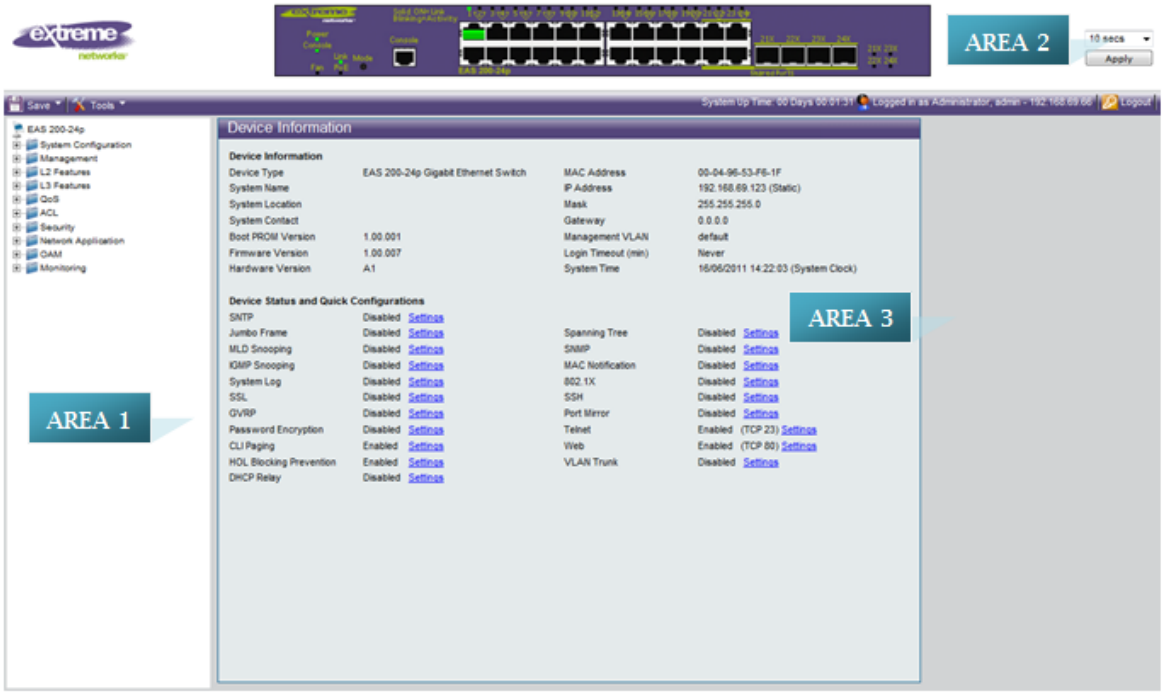
Web-based User Interface

The user interface provides access to various Switch configuration and management windows, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. Three distinct areas divide the user interface, as described in the table.

Figure 2: Main Web-Manager page



Area Number	Function
Area 1	Select the menu or window to display. Open folders and click the hyperlinked menu buttons and subfolders contained within them to display menus. Click the Extreme logo to go to the Extreme website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports, console and management port, showing port activity. Some management functions, including save, reboot, download and upload are accessible here.
Area 3	Presents switch information based on user selection and the entry of configuration data.

Web Pages

When connecting to the management mode of the Switch with a web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list of the main folders available in the Web interface:

- **System Configuration** - In this section the user will be able to configure features regarding the Switch's configuration.

- **Management** - In this section the user will be able to configure features regarding the Switch's management.
- **L2 Features** - In this section the user will be able to configure features regarding the Layer 2 functionality of the Switch.
- **L3 Features** - In this section the user will be able to configure features regarding the Layer 3 functionality of the Switch.
- **QoS** - In this section the user will be able to configure features regarding the Quality of Service functionality of the Switch.
- **ACL** - In this section the user will be able to configure features regarding the Access Control List functionality of the Switch.
- **Security** - In this section the user will be able to configure features regarding the Switch's security.
- **Network Application** - In this section the user will be able to configure features regarding network applications handled by the Switch.
- **OAM** - In this section the user will be able to configure features regarding the Switch's operations, administration and maintenance (OAM).
- **Monitoring** - In this section the user will be able to monitor the Switch's configuration and statistics.

NOTE

Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

2 System Configuration

CHAPTER

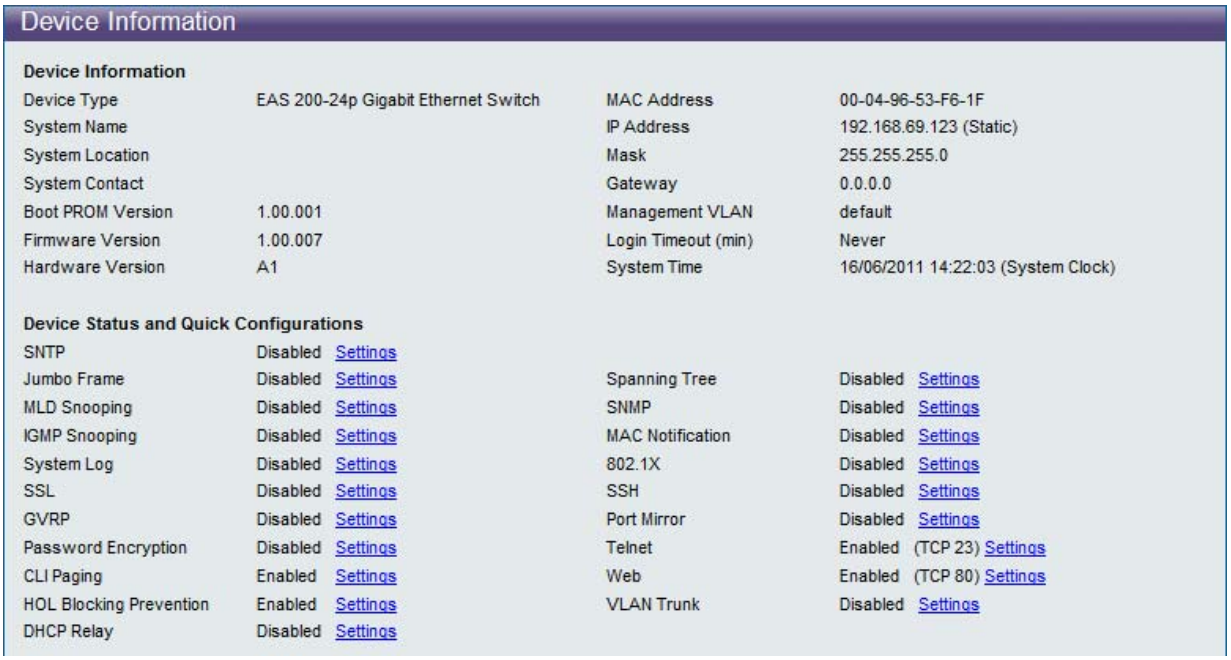
Device Information

This window contains the main settings for all the major functions for the Switch. It appears automatically when you log on to the Switch. To return to the Device Information window after viewing other windows, click the **EAS 200-24p** link.

The Device Information window shows the Switch's MAC Address (assigned by the factory and unchangeable), the Boot PROM Version, Firmware Version, Hardware Version, and many other important types of information. This is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their current global status.

Many functions are hyper-linked for easy access to enable quick configuration from this window.

Figure 3: Device Information window



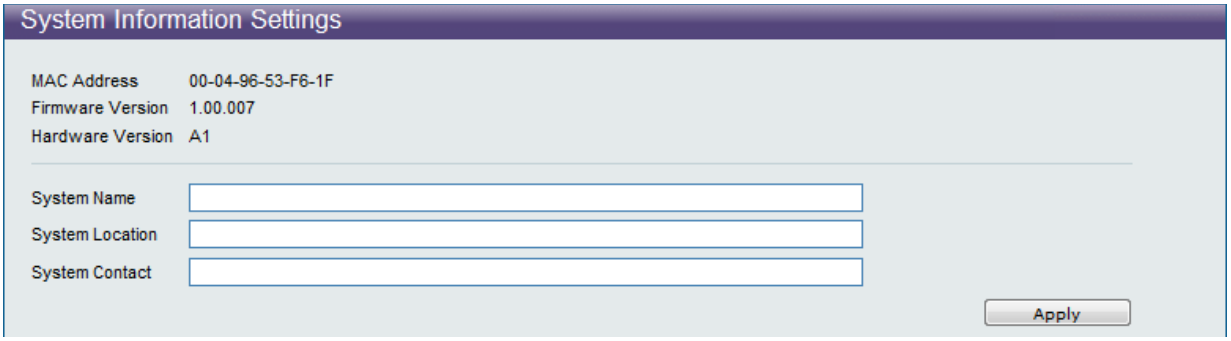
Click the **Settings** link to navigate to the appropriate feature page for configuration.

System Information Settings

The user can enter a **System Name, System Location, and System Contact** to aid in defining the Switch.

To view the following window, click **System Configuration > System Information Settings**, as show below:

Figure 4: System Information Settings window



The fields that can be configured are described below:

Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.

Click the **Apply** button to implement changes made.

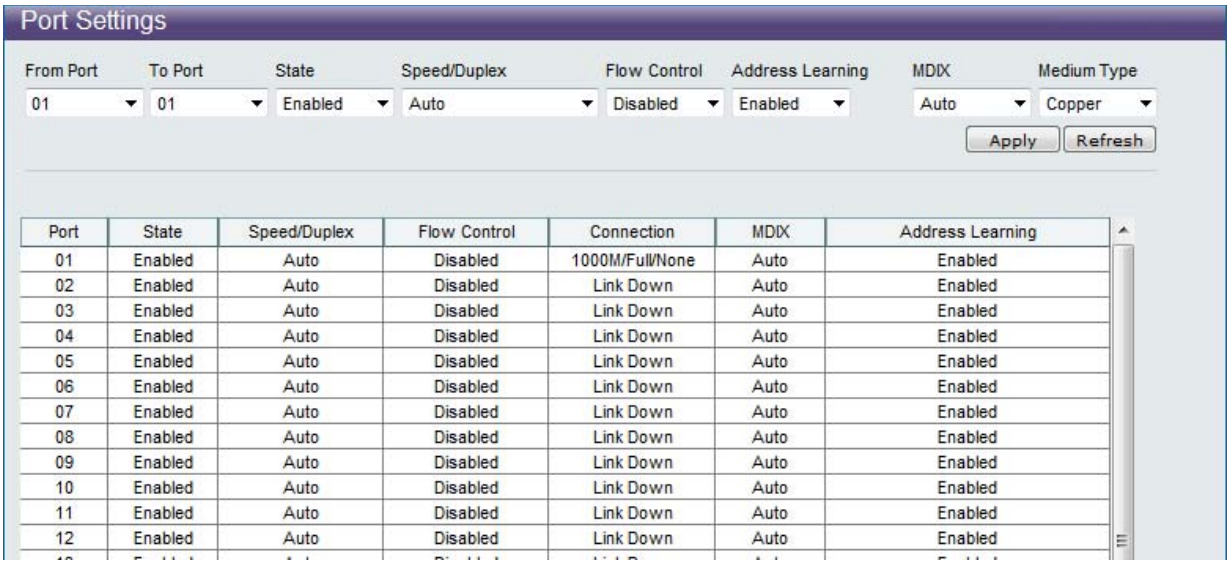
Port Configuration

Port Settings

This page used to configure the details of the switch ports.

To view the following window, click **System Configuration > Port Configuration > Port Settings**, as show below:

Figure 5: Port Settings window



To configure switch ports:

1 Choose the port or sequential range of ports using the From Port and To Port pull-down menus.

2 Use the remaining pull-down menus to configure the parameters described below:

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Toggle the State field to either enable or disable a given port or group of ports.

Parameter	Description
Speed/Duplex	Toggle the Speed/Duplex field to select the speed and full-duplex/half-duplex state of the port. *Auto* denotes auto-negotiation among 10, 100 and 1000 Mbps devices, in full- or half-duplex (except 1000 Mbps which is always full duplex). The *Auto* setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *10M Half*, *10M Full, 100M Half*, *100M Full*, *1000M Full_Master*, *1000M Full_Slave, and 1000M Full*. There is no automatic adjustment of port settings with any option other than *Auto*. The Switch allows the user to configure three types of gigabit connections; *1000M Full_Master*, *1000M Full_Slave*, and *1000M Full*. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The *1000M Full_Master* and *1000M Full_Slave* parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (*1000M Full_Master)* will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (*1000M Full_Slave)* uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for *1000M Full_Master*, the other side of the connection must be set for *1000M Full_Slave*. Any other configuration will result in a link down status for both ports.
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two. The default is *Disabled*.
Connection	Here the current connection speed will be displayed.
MDIX	*Auto* - Select auto for auto sensing of the optimal type of cabling. *Normal* - Select normal for normal cabling. If set to normal state, the port is in MDI mode and can be connected to a PC NIC using a straight-through cable or a port (in MDI mode) on another switch through a cross-over cable. *Cross* - Select cross for cross cabling. If set to cross state, the port is in MDIX mode, and can be connected to a port (in MDI mode) on another switch through a straight cable.
Address Learning	Enable or disable MAC address learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When address learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on Forwarding/Filtering for information on entering MAC addresses into the forwarding table. The default setting is *Enabled*.
Medium Type	If configuring the Combo ports, this defines the type of transport medium to be used.

Click the **Apply** button to implement changes made.

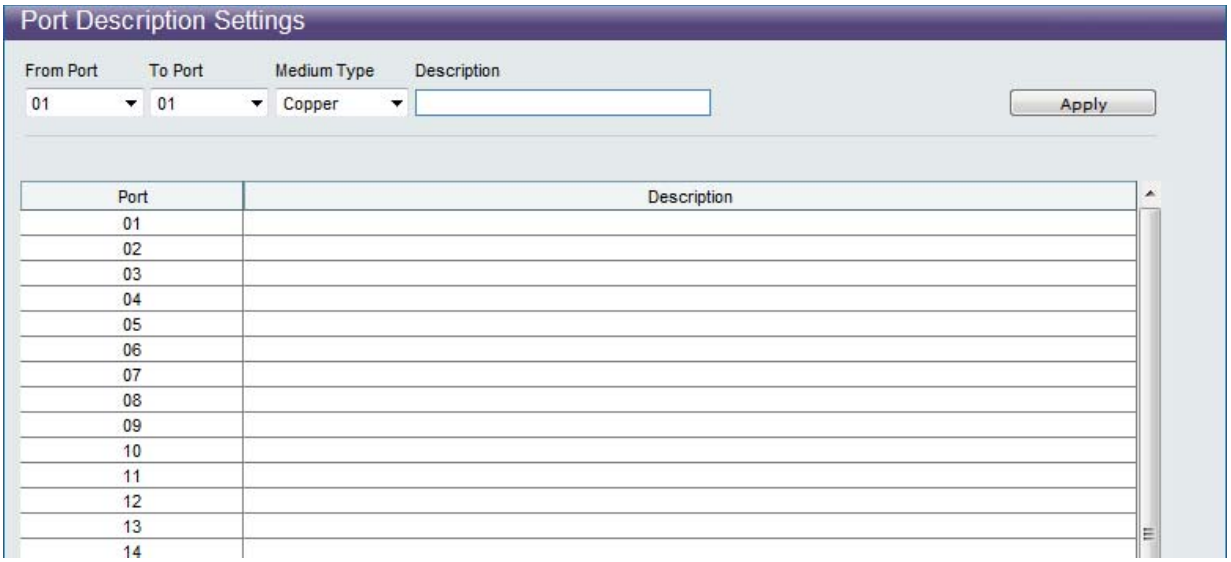
Click the **Refresh** button to refresh the display section of this page.

Port Description Settings

The Switch supports a port description feature where the user may name various ports.

To view the following window, click **System Configuration > Port Configuration > Port Description Settings**, as show below:

Figure 6: Port Description Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Medium Type	Specify the medium type for the selected ports. If configuring the Combo ports, the Medium Type defines the type of transport medium to be used, whether *Copper* or *Fiber.*
Description	Users may then enter a description for the chosen port(s).

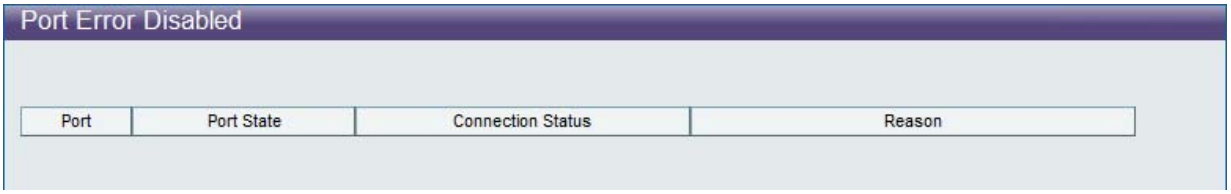
Click the **Apply** button to implement changes made.

Port Error Disabled

The following window displays the information about ports that have been disconnected by the Switch when a packet storm occurs or a loop was detected.

To view the following window, click **System Configuration > Port Configuration > Port Error Disabled**, as show below:

Figure 7: Port Error Disabled



The fields that can be displayed are described below:

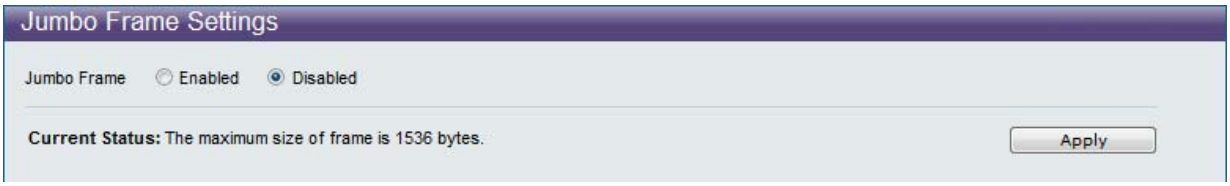
Parameter	Description
Port	Display the port that has been error disabled.
Port State	Describe the current running state of the port, whether enabled or disabled.
Connection Status	Display the uplink status of the individual ports, whether enabled or disabled.
Reason	Describe the reason why the port has been error-disabled, such as it has become a shutdown port for storm control.

Jumbo Frame Settings

The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 13312 bytes.

To view the following window, click **System Configuration > Port Configuration > Jumbo Frame Settings**, as show below:

Figure 8: Jumbo Frame Settings window



The fields that can be configured are described below:

Parameter	Description
Jumbo Frame	Use the radio buttons to enable or disable the Jumbo Frame function on the Switch. The default is Disabled. When disabled, the maximum frame size is 1536 bytes. When enabled, the maximum frame size is 13312 bytes.

Click the **Apply** button to implement changes made.

PoE

The EAS 200-24p Switch support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. All ports can support PoE up to 30W. Ports 1-24 can supply about 48 VDC power to Powered Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. The Switch follows the standard PSE (Power Sourcing Equipment) pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The Switches work with all Extreme 802.3af capable devices.

The Switch includes the following PoE features:

- Auto-discovery recognizes the connection of a PD (Powered Device) and automatically sends power to it.
- The Auto-disable feature occurs under two conditions: firstly, if the total power consumption exceeds the system power limit; and secondly, if the per port power consumption exceeds the per port power limit.

- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

Based on 802.3af/at PDs receive power according to the following classification:

Class	Maximum power available to PD
0	15.4W
1	4.0W
2	7.0W
3	15.4W
4	15.4W

PSE provides power according to the following classification:

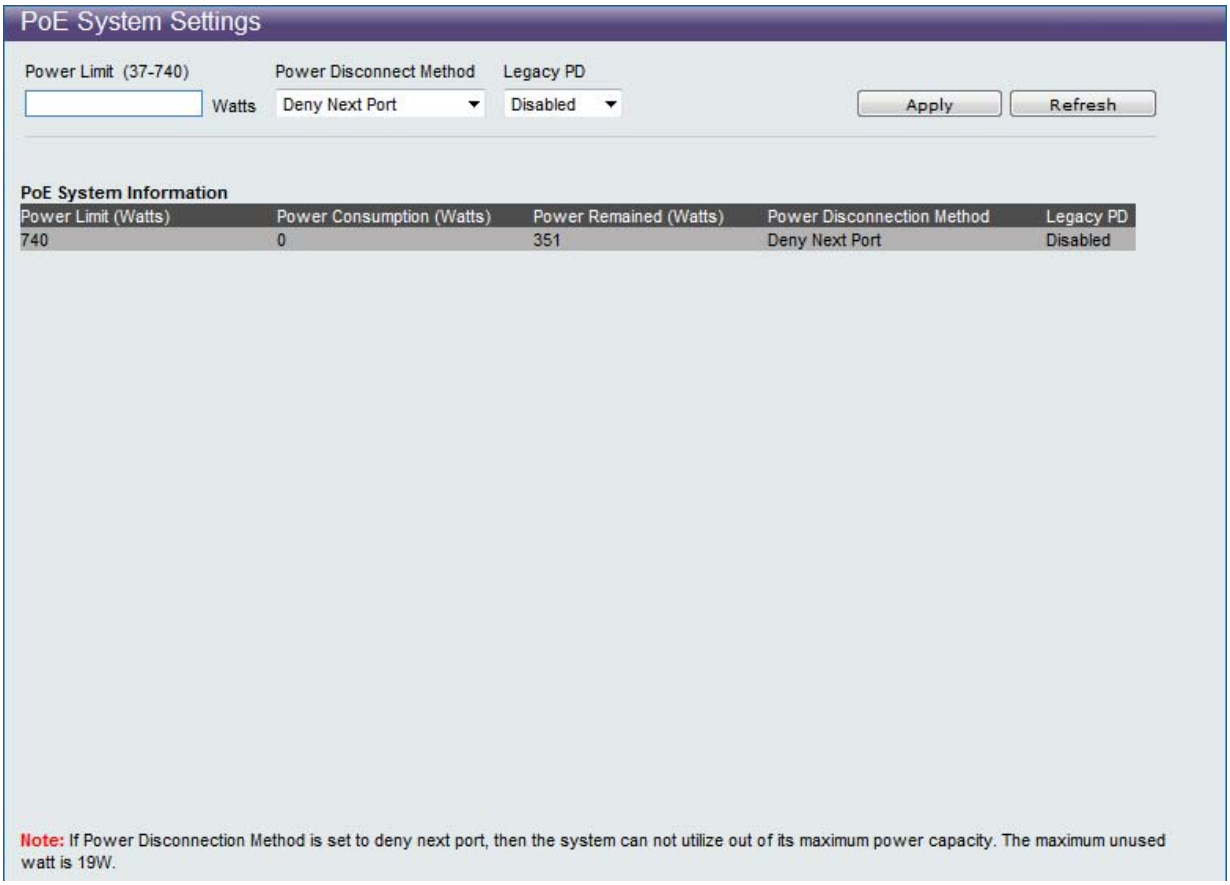
Class	Max power used by PSE
0	16.2W
1	4.2W
2	7.4W
3	16.2W
User define	31.2W

To configure the PoE features on the Switch, click **System Configuration > PoE**. The **PoE System Settings** window is used to assign a power limit and power disconnect method for the whole PoE system. To configure the **Power Limit** for the PoE system, enter a value between 1W and 370W for the Switch in the Power Limit field. When the total consumed power exceeds the power limit, the PoE controller (located in the PSE) disconnects the power to prevent overloading the power supply.

PoE System Settings

To view the following window, click **System Configuration > PoE > PoE System Settings**, as show below:

Figure 9: PoE System Settings window



The following parameters can be configured:

Parameter	Description
Power Limit (37-740)	Sets the limit of power to be used from the Switch's power source to PoE ports. The user may configure a Power Limit between 37W and 740W for the Switch. The default setting is 740W.
Power Disconnect Method	The PoE controller uses either *Deny Next Port* or *Deny Low Priority Port* to offset the power limit being exceeded and keeps the Switch's power at a usable level. Use the drop down menu to select a **Power Disconnect Method**. The default Power Disconnect Method is *Deny Next Port*. Both Power Disconnection Methods are described below: *Deny Next Port* – After the power limit has been exceeded, the next port attempting to power up is denied, regardless of its priority. If Power Disconnection Method is set to *Deny Next Port*, the system cannot utilize out of its maximum power capacity. The maximum unused watt is 19W. *Deny Low Priority Port* – After the power limit has been exceeded, the next port attempting to power up causes the port with the lowest priority to shut down so as to allow the high-priority and critical priority ports to power up.

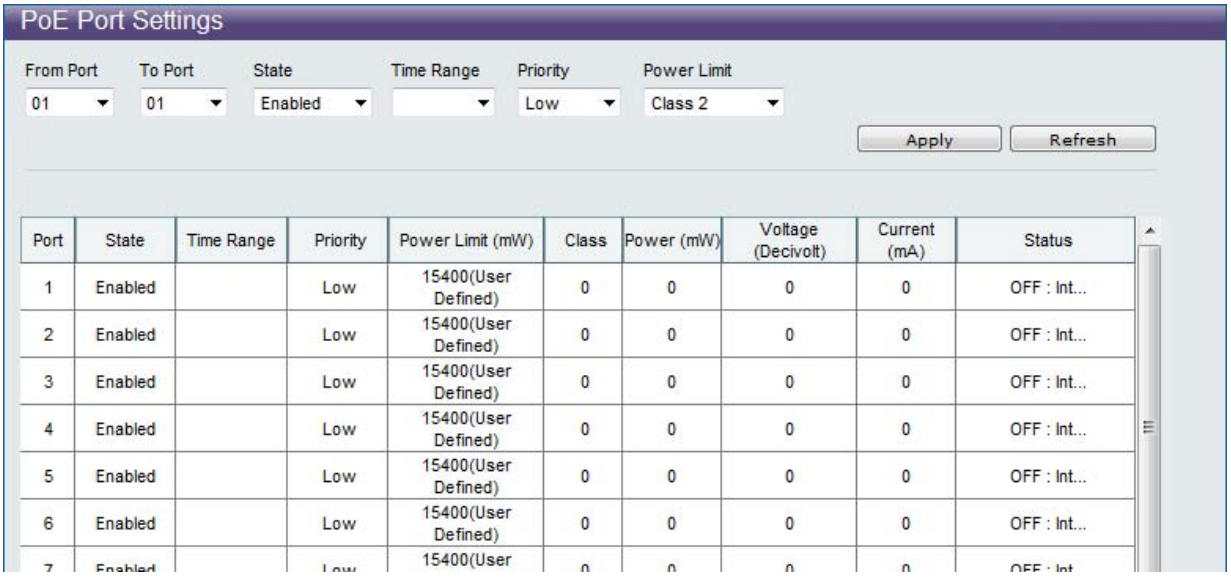
Parameter	Description
Legacy PD	Use the drop-down menu to enable or disable detecting legacy PDs signal.

Click **Apply** to implement changes made.

PoE Port Settings

To view the following window, click **System Configuration > PoE > PoE Port Settings**, as show below:

Figure 10: PoE Port Settings window



The following parameters can be configured:

Parameter	Description
From Port / To Port	Select a range of ports from the pull-down menus to be enabled or disabled for PoE.
State	Use the pull-down menu to enable or disable ports for PoE.
Time Range	Select a range of the time to the port set as POE. If Time Range is configured, the power can only be supplied during the specified period of time.
Priority	Use the pull-down menu to select the priority of the PoE ports. Port priority determines the priority which the system attempts to supply the power to the ports. There are three levels of priority that can be selected, *Critical*, *High*, and *Low*. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the order of supplying power. Whether the disconnect method is set to deny low priority port, the priority of each port will be used by the system to manage the supply of power to ports.

Parameter	Description
Power Limit	This function is used to configure the per-port power limit. If a port exceeds its power limit, it will shut down. Based on 802.3af/802.3at, there are different PD classes and power consumption ranges; • Class 0 – 0.44~15.4W • Class 1 – 0.44~4.0W • Class 2 – 4~7.0W • Class 3 – 7~15.4W • Class 4 – 15.4W The following is the power limit applied to the port for these five classes. For each class, the power limit is a little more than the power consumption range for that class. This takes into account any power loss on the cable. Thus, the following are the typical values; • *Class 0* – 16200mW • *Class 1* – 4200mW • *Class 2* – 7400mW • *Class 3* – 16200mW • *User Define* – 35000mW

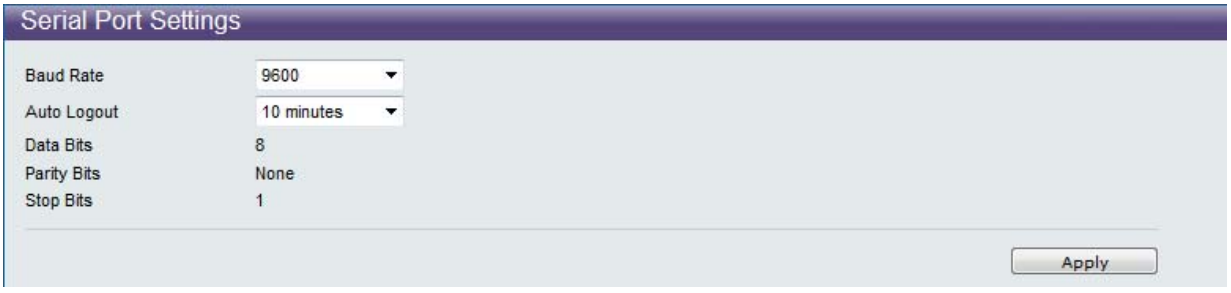
Click **Apply** to implement changes made. The port status of all PoE configured ports is displayed in the table in the bottom half of the screen shown above.

Serial Port Settings

This window allows the user to adjust the Baud Rate and the Auto Logout values.

To view the following window, click **System Configuration > Serial Port Settings**, as show below:

Figure 11: Serial Port Settings window



The fields that can be configured are described below:

Parameter	Description
Baud Rate	Specify the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, *9600*, *19200*, *38400* and *115200*. For a connection to the Switch using the console port, the baud rate must be set to *9600*, which is the default setting.

Parameter	Description
Auto Logout	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: *2, 5, 10, 15 minutes* or *Never*. The default setting is *10 minutes*.
Data Bits	Display the data bits used for the serial port connection.
Parity Bits	Display the parity bits used for the serial port connection.
Stop Bits	Display the stop bits used for the serial port connection.

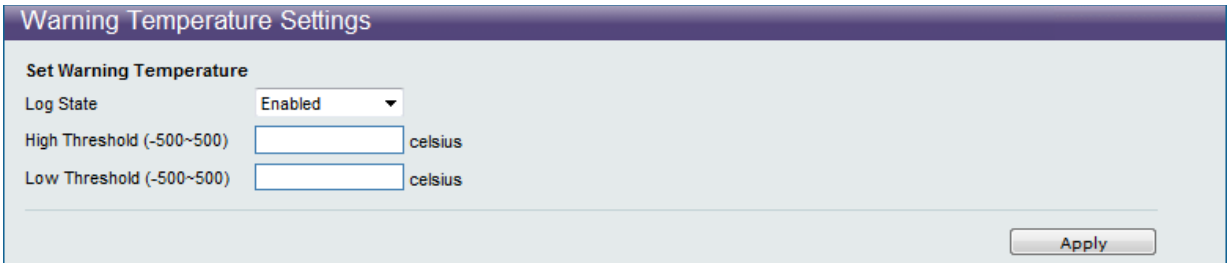
Click the **Apply** button to implement changes made.

Warning Temperature Settings

This window allows the user to configure the system warning temperature parameters.

To view the following window, click **System Configuration > Warning Temperature Settings**, as show below:

Figure 12: Warning Temperature Settings window



The fields that can be configured are described below:

Parameter Description

Parameter	Description
Log State	Use the drop-down menu to enable or disable the log state option of the warning temperature setting.
High Threshold	Enter the high threshold value of the warning temperature setting.
Low Threshold	Enter the low threshold value of the warning temperature setting.

Click the **Apply** button to implement changes made.

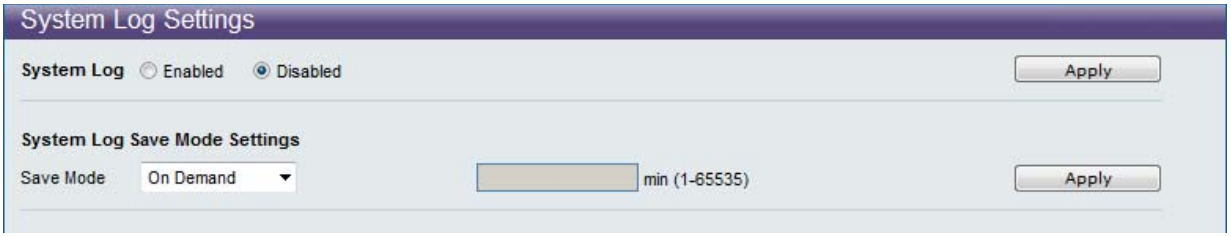
System Log configuration

System Log Settings

The Switch allows users to choose a method for which to save the switch log to the flash memory of the Switch.

To view the following window, click **System Configuration > System Log Configuration > System Log Settings**, as show below:

Figure 13: System Log Settings window



The fields that can be configured are described below:

Parameter	Description
System Log	Use the radio buttons to enable or disable the system log settings. Click the **Apply** button to accept the changes made.
Save Mode	Use the pull-down menu to choose the method for saving the switch log to the flash memory. The user has three options: *On Demand* – Users who choose this method will only save log files when they manually tell the Switch to do so, either using the Save Log link in the Save folder. *Time Interval* – Users who choose this method can configure a time interval by which the Switch will save the log files, in the box adjacent to this configuration field. The user may set a time between 1 and 65535 minutes. *Log Trigger* – Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.

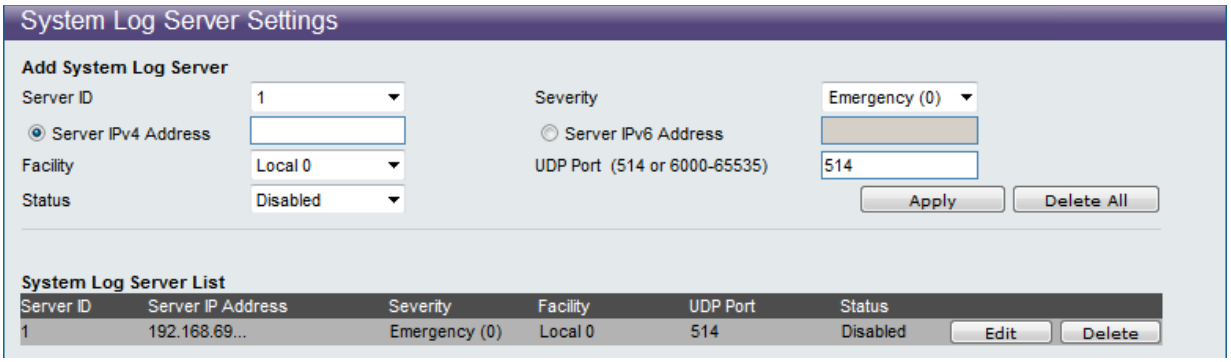
Click the **Apply** button to accept the changes made.

System Log Server Settings

The Switch can send System log messages to up to four designated servers using the System Log Server.

To view the following window, click **System Configuration > System Log Configuration > System Log Server Settings**, as show below:

Figure 14: System Log Server Settings



The fields that can be configured are described below:

Parameter	Description
Server ID	Syslog server settings index (1 to 4).
Server IPv4 Address	The IPv4 address of the Syslog server.
Server IPv6 Address	The IPv6 address of the Syslog server.
UDP Port	Type the UDP port number used for sending Syslog messages. The default is 514.
Severity	Use the drop-down menu to select the higher level of messages that will be sent. All messages which level is higher than selecting level will be sent. The options are *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Informational* and *Debug*.
Facility	Use the drop-down menu to select *Local 0*, *Local 1*, *Local 2*, *Local 3*, *Local 4*, *Local 5*, *Local 6*, or *Local 7*.
Status	Choose Enabled or Disabled to activate or deactivate.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

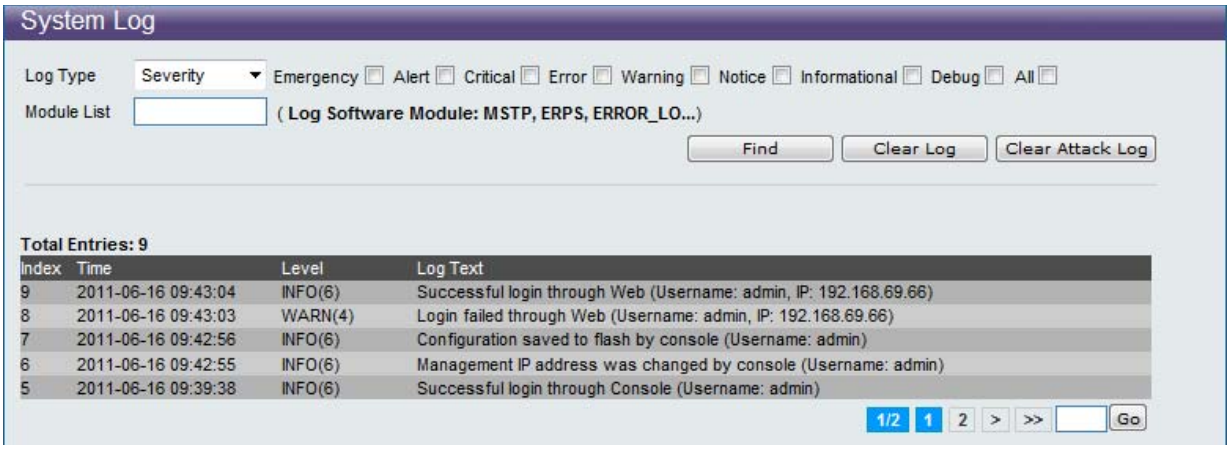
Click the **Delete All** button to remove all servers configured.

System Log

Users can view and delete the local history log as compiled by the Switch's management agent.

To view the following window, click **System Configuration > System Log Configuration > System Log**, as show below:

Figure 15: System Log window



The Switch can record event information in its own log. Click **Go** to go to the next page of the **System Log** window.

The fields that can be configured are described below:

Parameter	Description
Log Type	In the drop-down menu the user can select the log type that will be displayed. *Severity* - When selecting *Severity* from the drop-down menu, a secondary tick must be made. Secondary ticks are **Emergency, Alert, Critical, Error, Warning, Notice, Informational** and **Debug**. To view all information in the log, simply tick the **All** check box. *Module List* - When selecting *Module List*, the module name must be manually entered. Available modules are MSTP, ERPS, ERROR_LOG, and CFM_EXT. *Attack Log* - When selecting *Attack Log* all attacks will be listed.
Index	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Display the time in days, hours, minutes, and seconds since the Switch was last restarted.
Level	Display the level of the log entry.
Log Text	Display text describing the event that triggered the history log entry.

Click the **Find** button to display the log in the display section according to the selection made.

Click the **Clear Log** button to clear the entries from the log in the display section.

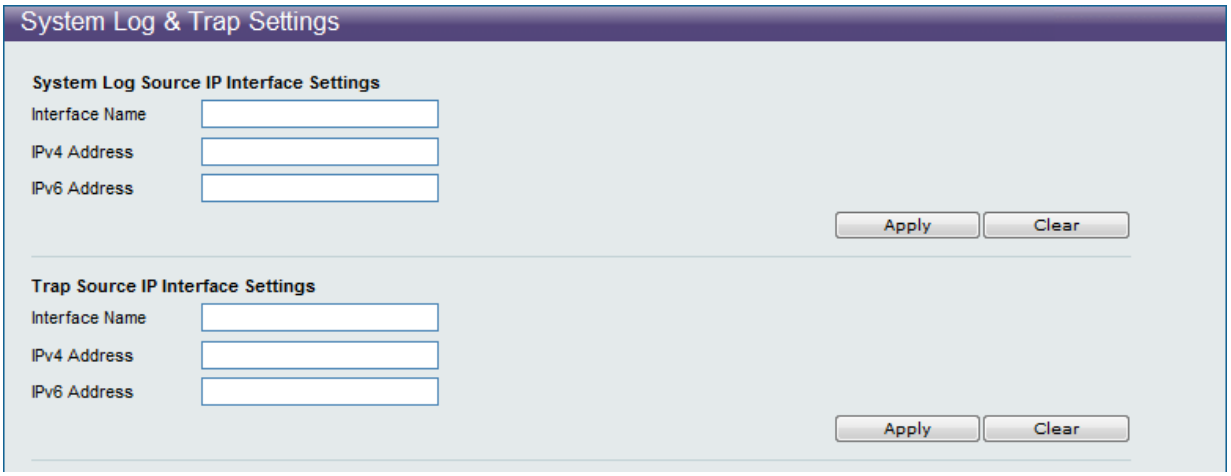
Click the **Clear Attack Log** button to clear the entries from the attack log in the display section.

System Log & Trap Settings

The Switch allows users to configure the system log source IP interface addresses here.

To view the following window, click **System Configuration > System Log Configuration > System Log & Trap Settings**, as show below:

Figure 16: System Log & Trap Settings window



The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP interface name used.
IPv4 Address	Enter the IPv4 address used.
IPv6 Address	Enter the IPv6 address used.

Click the **Apply** button to accept the changes made.

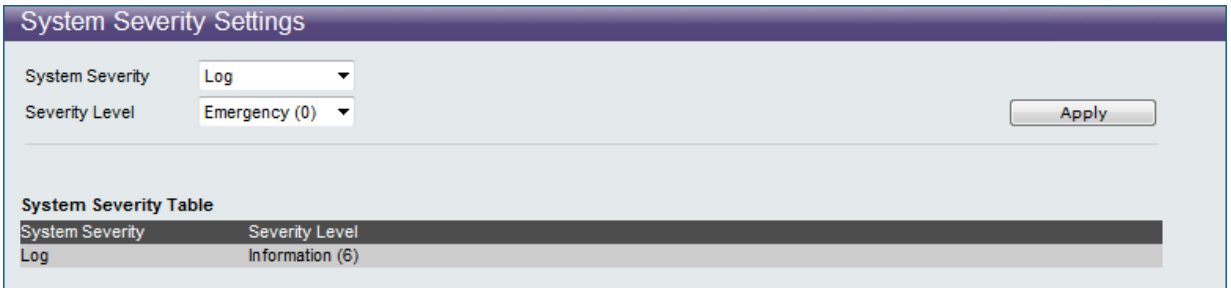
Click the **Clear** button to clear all the information entered in the fields.

System Severity Settings

The Switch can be configured to allow alerts be logged or sent as a trap to an SNMP agent. The level at which the alert triggers either a log entry or a trap message can be set as well. Use the System Severity Settings window to set the criteria for alerts. The current settings are displayed below the System Severity Table.

To view the following window, click **System Configuration > System Log Configuration > System Severity Settings**, as show below:

Figure 17: System Severity Settings window



The fields that can be configured are described below:

Parameter	Description
System Severity	Choose how the alerts are used from the drop-down menu. Select *Log* to send the alert of the Severity Type configured to the Switch's log for analysis.
Severity Level	This drop-down menu allows you to select the level of messages that will be sent. The options are *Emergency (0)*, *Alert (1)*, *Critical (2)*, *Error (3)*, *Warning (4)*, *Notice (5)*, *Information (6)* and *Debug (7)*.

Click the **Apply** button to accept the changes made.

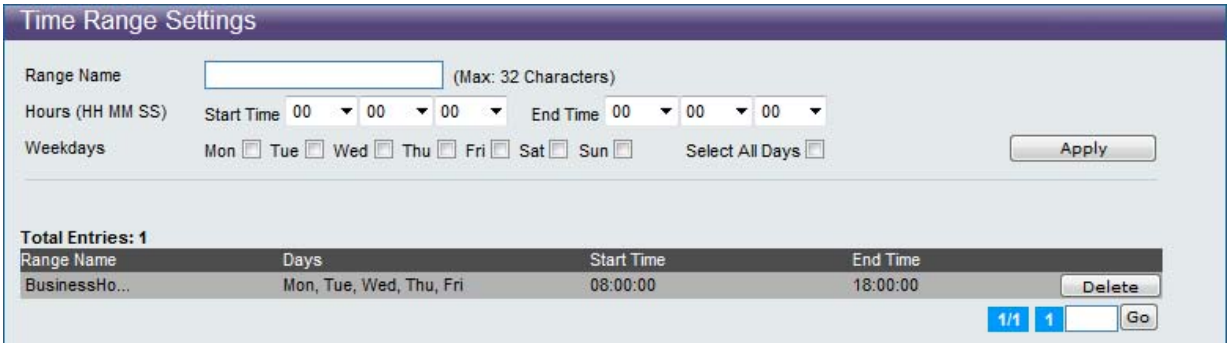
Time Range Settings

Time range is a time period that the respective function will take an effect on, such as ACL. For example, the administrator can configure the time-based ACL to allow users to surf the Internet on every Saturday and every Sunday, meanwhile to deny users to surf the Internet on weekdays.

The user may enter up to 64 time range entries on the Switch.

To view the following window, click **System Configuration > Time Range Settings**, as show below:

Figure 18: Time Range Settings window



The fields that can be configured are described below:

Parameter	Description
Range Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the Access Profile table to identify the access profile and associated rule to be enabled during this time range.
Hours	This parameter is used to set the time in the day that this time range is to be enabled using the following parameters: *Start Time* - Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. *End Time* - Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system.
Weekdays	Use the check boxes to select the corresponding days of the week that this time range is to be enabled. Tick the Select All Days check box to configure this time range for every day of the week.

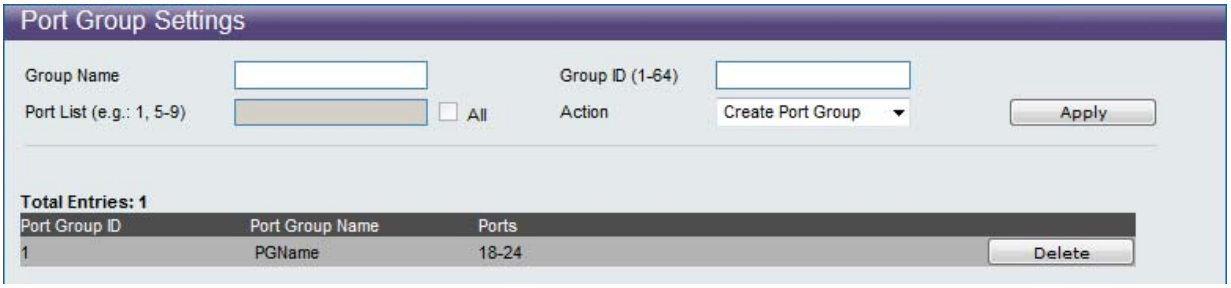
Click the **Apply** button to accept the changes made. Current configured entries will be displayed in the **Time Range Information** table in the bottom half of the window shown above.

Port Group Settings

This window is used to create port groups, and add or delete ports from the port groups.

To view the following window, click **System Configuration > Port Group Settings**, as show below:

Figure 19: Port Group Settings window



The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the name of a port group.
Group ID (1-64)	Enter the ID of a port group
Port List	Enter a port or list of ports. Tick the **All** check box to apply to all ports.
Action	Use the drop-down menu to select *Create Port Group*, *Add Ports* or *Delete Ports*.

Click the **Apply** button to accept the changes made.

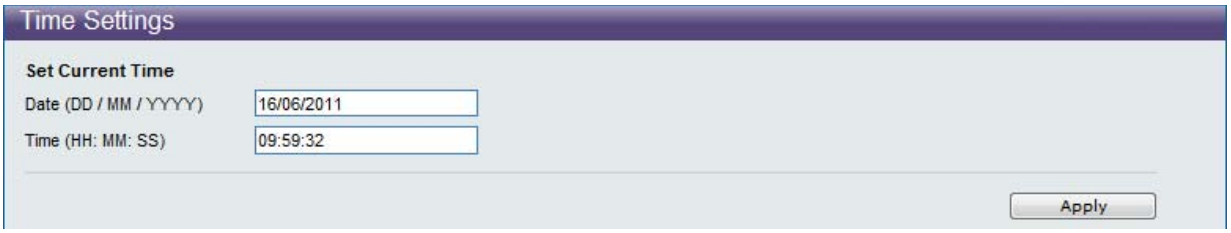
Click the **Delete** button to remove the specific entry.

Time Settings

Users can configure the time settings for the Switch.

To view the following window, click **System Configuration > Time Settings**, as show below:

Figure 20: Time Settings window



The fields that can be configured are described below:

Parameter	Description
Date (DD/MM/YYYY)	Enter the current day, month, and year to update the system clock.
Time (HH: MM: SS)	Enter the current time in hours, minutes, and seconds.

Click the **Apply** button to accept the changes made.

User Accounts Settings

The Switch allows the control of user privileges.

To view the following window, click **System Configuration > User Accounts Settings**, as show below:

Figure 21: User Accounts Settings window

To add a new user, type in a User Name and New Password and retype the same password in the Confirm New Password field. Choose the level of privilege (Admin, Operator, Power User or User) from the Access Right drop-down menu.

Management	Admin	Operator	Power User	User
Configuration	Read/Write	Read/Write–partly	Read/Write–partly	No
Network Monitoring	Read/Write	Read/Write	Read-only	Read-only
Community Strings and Trap Stations	Read/Write	Read-only	Read-only	Read-only
Update Firmware and Configuration Files	Read/Write	No	No	No
System Utilities	Read/Write	Read-only	Read-only	Read-only
Factory Reset	Read/Write	No	No	No
User Account Management				
Add/Update/Delete User Accounts	Read/Write	No	No	No
View User Accounts	Read/Write	No	No	No

The fields that can be configured are described below:

Parameter	Description
User Name	Enter a new user name for the Switch.
Password	Enter a new password for the Switch.
Confirm Password	Re-type in a new password for the Switch.
Access Right	Specify the access right for this user.
Encryption	Specifies that encryption will be applied to this account. Option to choose from are *Plain Text*, and *SHA-1*.

Click the **Apply** button to accept the changes made.

CAUTION

In case of lost passwords or password corruption, please refer to the appendix chapter entitled, “Password Recovery Procedure,” which will guide you through the steps necessary to resolve this issue.

NOTE

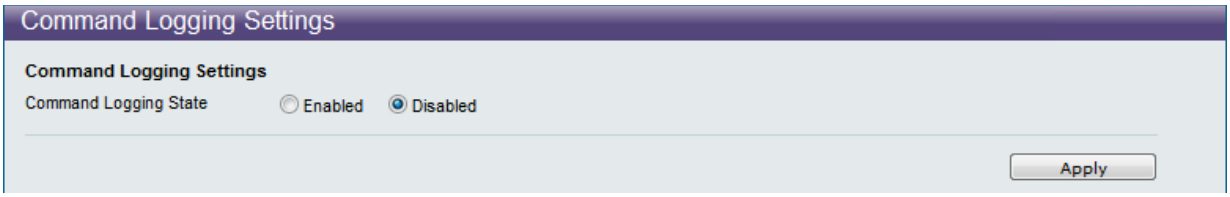
The username and password should be less than 16 characters.

Command Logging Settings

This window is used to enable or disable the command logging settings.

To view this window, click **System Configuration** > **Command Logging Settings**, as shown below:

Figure 22: Command Logging Settings window



The fields that can be configured are described below:

Parameter	Description
Command Logging State	Use the radio buttons to enable or disable the function.

Click the **Apply** button to accept the changes made.

NOTE

When the switch is under the booting procedure, all configuration commands will not be logged. When the user uses AAA authentication to logged in, the user name should not be changed if the user has used the Enable Admin function to replace its privilege.

3 Management

CHAPTER

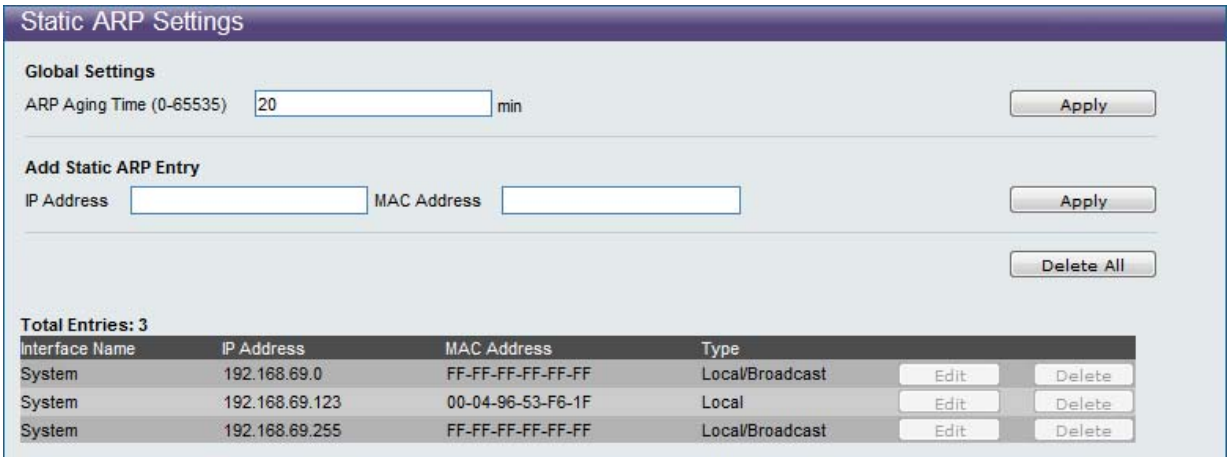
ARP

Static ARP Settings

The Address Resolution Protocol is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify, and delete ARP information for specific devices. Static entries can be defined in the ARP table. When static entries are defined, a permanent entry is entered and is used to translate IP addresses to MAC addresses.

To view the following window, click **Management > ARP > Static ARP Settings**, as show below:

Figure 23: Static ARP Settings window



The fields that can be configured are described below:

Parameter	Description
ARP Aging Time (0-65535)	The ARP entry age-out time, in minutes. The default is *20* minutes.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

Click the **Apply** button, located in the **Global Settings** section to accept the changes made in this section.

Click the **Apply** button, located in the **Add Static ARP Entry** section to accept the changes made in this section.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Proxy ARP Settings

The Proxy ARP (Address Resolution Protocol) feature of the Switch will allow the Switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP responder. Therefore, the Switch can then route packets to the intended destination without configuring static routing or a default gateway.

The host, usually a layer 3 switch, will respond to packets destined for another device. For example, if hosts A and B are on different physical networks, B will not receive ARP broadcast requests from A and therefore cannot respond. Yet, if the physical network of A is connected by a router or layer 3 switch to B, the router or Layer 3 switch will see the ARP request from A.

This lovcal proxy ARP function allows the Switch to respond to the proxy ARP, if the source IP and destination IP are in the same interface.

To view the following window, click **Management > ARP > Proxy ARP Settings**, as show below:

Figure 24: Proxy ARP Settings window

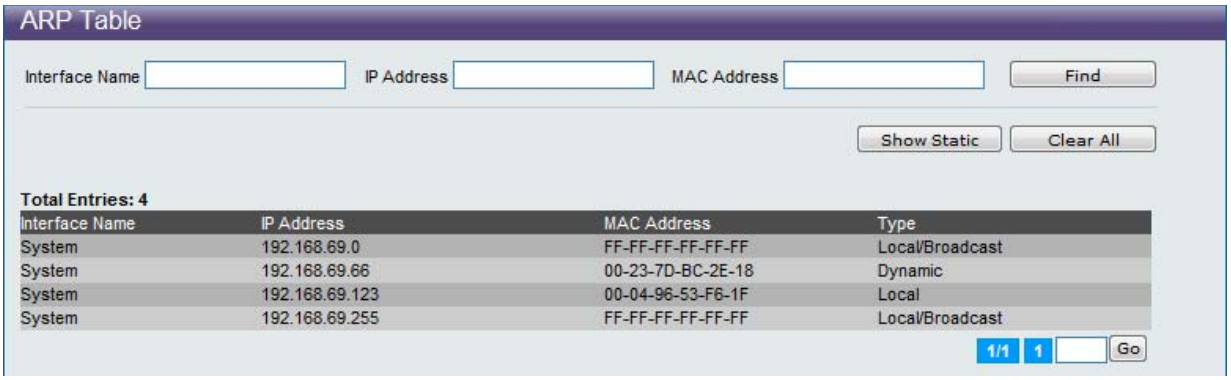
Click the **Edit** button to re-configure the specific entry and select the proxy ARP state of the IP interface. By default, both the **Proxy ARP State** and **Local Proxy ARP State** are disabled.

ARP Table

Users can display current ARP entries on the Switch.

To view the following window, click **Management > ARP > ARP Table**, as show below:

Figure 25: ARP Table window



The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter or view the Interface name used.
IP Address	Enter or view the IP Address used.
MAC Address	Enter or view the MAC Address used.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Static** button to display only the static entries in the display table.

Click the **Clear All** button to remove all the entries listed in the table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

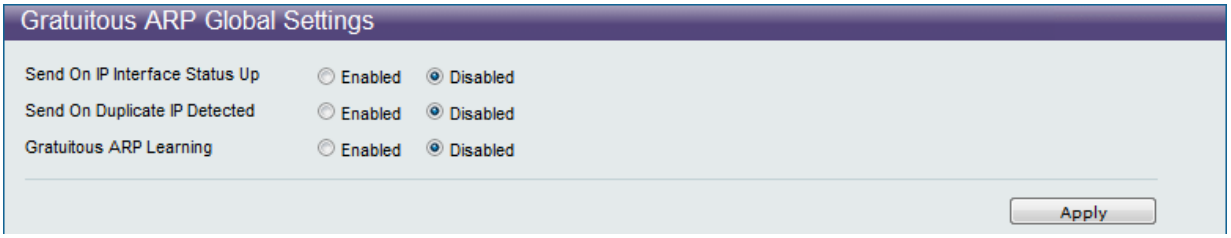
Gratuitous ARP

Gratuitous ARP Global Settings

The user can enable or disable the gratuitous ARP global settings here.

To view the following window, click **Management > Gratuitous ARP > Gratuitous ARP Global Settings**, as show below:

Figure 26: Gratuitous ARP Global Settings Window



The fields that can be configured are described below:

Parameter	Description
Send On IP Interface Status Up	The command is used to enable/disable sending of gratuitous ARP request packet while the IPIF interface become up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled, and only one gratuitous ARP packet will be broadcast.
Send On Duplicate IP Detected	The command is used to enable/disable the sending of gratuitous ARP request packet while a duplicate IP is detected. By default, the state is disabled. For this command, the duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that match the system's own IP address. In this case, the system knows that somebody out there uses an IP address that is conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packets for this duplicate IP address.
Gratuitous ARP Learning	Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The command is used to enable/disable learning of ARP entry in ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. By default, the state is Disabled status.

Click the **Apply** button to accept the changes made.

NOTE

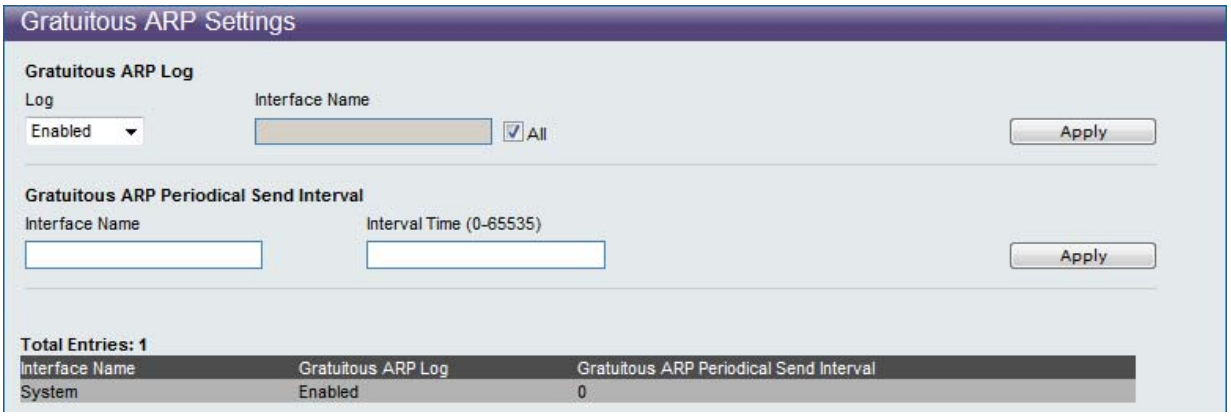
With the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet.

Gratuitous ARP Settings

The user can configure the IP interface's gratuitous ARP parameter.

To view the following window, click **Management > Gratuitous ARP > Gratuitous ARP Settings**, as show below:

Figure 27: Gratuitous ARP Settings window



The fields that can be configured are described below:

Parameter	Description
Log	Use the drop-down menu to enable or disable the logging option. By default the event log is enabled.
Interface Name	Enter the interface name of the Layer 3 interface. Select **All** to enable or disable gratuitous ARP trap or log on all interfaces.
Interval Time	Enter the periodically send gratuitous ARP interval time in seconds. 0 means that gratuitous ARP request will not be sent periodically. By default the interval time is 0.

Click the **Apply** button, located in the **Gratuitous ARP Trap/Log** section to accept the changes made in this section.

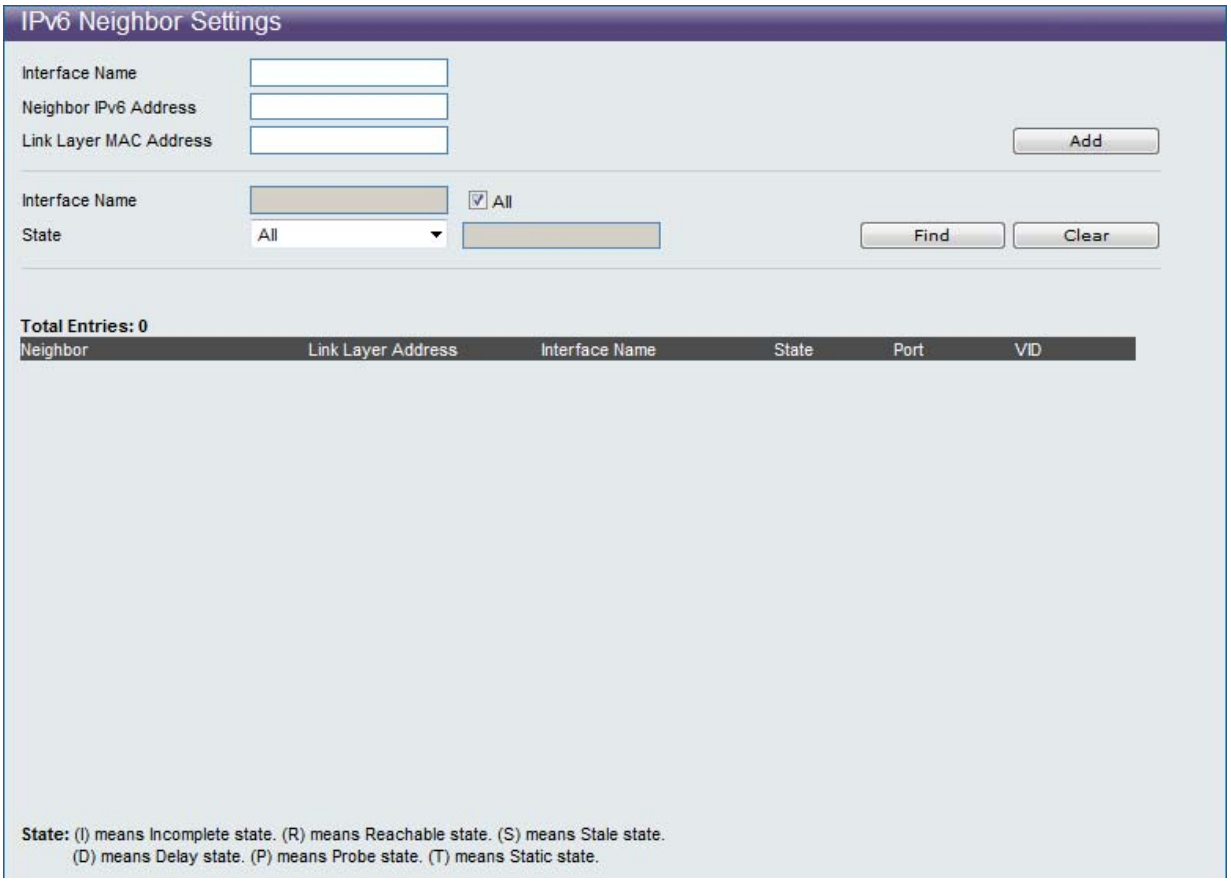
Click the **Apply** button, located in the **Gratuitous ARP Periodical Send Interval** section to accept the changes made in this section.

IPv6 Neighbor Settings

The user can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

To view the following window, click **Management > IPv6 Neighbor Settings**, as show below:

Figure 28: IPv6 Neighbor Settings



The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the interface name of the IPv6 neighbor.
Neighbor IPv6 Address	Enter the neighbor IPv6 address.
Link Layer MAC Address	Enter the link layer MAC address.
Interface Name	Enter the name of the IPv6 neighbor. Tick the **All** check box to search for all current interfaces on the Switch.
State	Use the drop-down menu to select All, Address, Static, or Dynamic. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information entered in the fields.

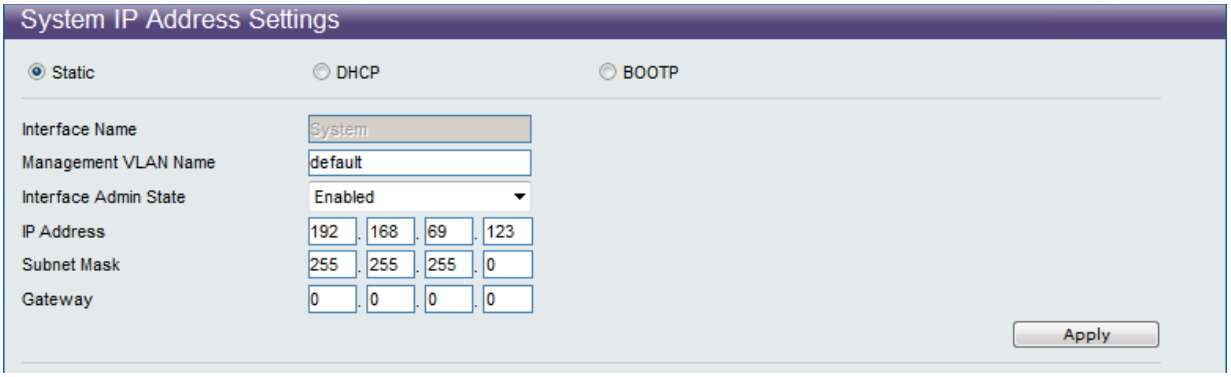
IP Interface

System IP Address Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. The Web manager will display the Switch's current IP settings.

To view the following window, click **Management > IP Interface > System IP Address Settings**, as show below:

Figure 29: System IP Address Settings window



The fields that can be configured are described below:

Parameter	Description
Static	Allow the entry of an IP address, subnet mask, and a default gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between *0* and *255*. This address should be a unique address on the network assigned for use by the network administrator.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.

The following table will describe the fields that are about the **System** Interface.

Parameter	Description
Interface Name	Display the System interface name.

Parameter	Description
Management VLAN Name	This allows the entry of a VLAN name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via Web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the **Trusted Host** window (**Security > Trusted Host)**. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Trusted Host table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP addresses are assigned.
Interface Admin State	Use the drop-down menu to enable or disable the configuration on this interface. If the state is disabled, the IP interface cannot be accessed.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between *0* and *255*. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

Click the **Apply** button to accept the changes made.

Interface Settings

Users can display the Switch's current IP interface settings.

To view the following window, click **Management > IP Interface > Interface Settings**, as show below:

Figure 30: Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the IP interface to search for.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **IPv4 Edit** button to edit the IPv4 settings for the specific entry.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

Click the **IPv6 Edit** button to edit the IPv6 settings for the specific entry.

Click the **Delete** button to remove the specific entry.

NOTE

To create IPv6 interfaces, the user has to create an IPv4 interface then edit it to IPv6.

Click the **Add** button to see the following window.

Figure 31: IPv4 Interface Settings window

The fields that can be configured are described below:

Parameter	Description
IP Interface Name	Enter the name of the IP interface being created.
IPv4 Address	Enter the IPv4 address used.
Subnet Mask	Enter the IPv4 subnet mask used.
VLAN Name	Enter the VLAN Name used.
Interface Admin State	Use the drop-down menu to enable or disable the Interface Admin State.
Secondary Interface	Tick the check box to use this Interface as a Secondary Interface. When the primary IP is not available, the VLAN will switch to the secondary interface. It will switch back when the primary IP was recovered.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **IPv4 Edit** button to see the following window.

Figure 32: IPv4 Interface Settings – Edit window

The fields that can be configured are described below:

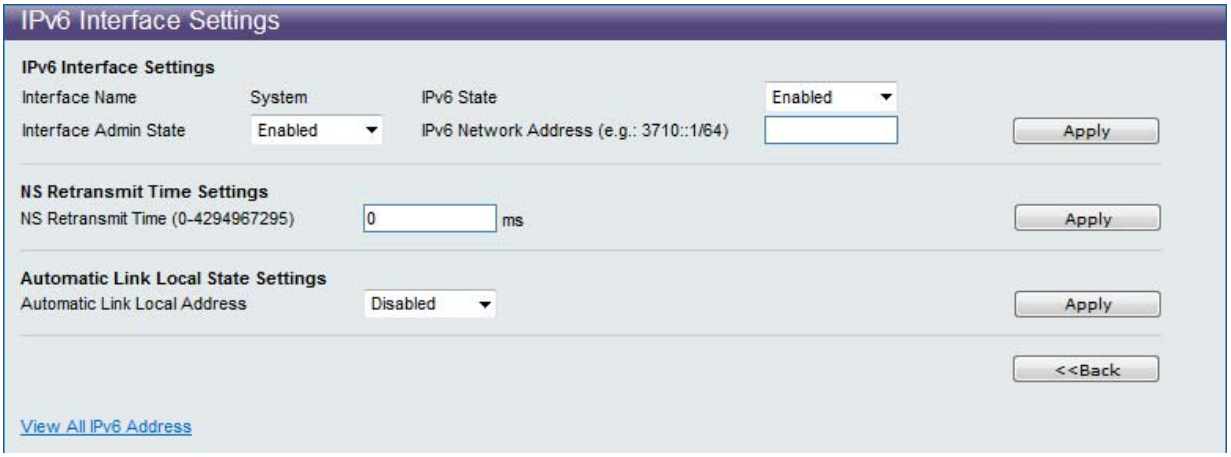
Parameter	Description
Get IP From	Use the drop-down menu to specify the method that this Interface uses to acquire an IP address.
Interface Name	Enter the name of the IP interface being configured.
IPv4 Address	Enter the IPv4 address used.
Subnet Mask	Enter the IPv4 subnet mask used.
VLAN Name	Enter the VLAN Name used.
IPv4 State	Use the drop-down menu to enable or disable IPv4 State.
Interface Admin State	Use the drop-down menu to enable or disable the Interface Admin State.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **IPv6 Edit** button to see the following window.

Figure 33: IPv6 Interface Settings window



The fields that can be configured are described below:

Parameter	Description
Interface Name	Here the IPv6 interface name is displayed
IPv6 State	Here the user can select to enable or disable IPv6 State.
Interface Admin State	Here the user can select to enable or disable the Interface Admin State.
IPv6 Network Address	Here the user can enter the neighbor's global or local link address.
NS Retransmit Time	Enter the Neighbor solicitation's retransmit timer in millisecond here. It has the same value as the RA retransmit time in the config ipv6 nd ra command. If this field is configured, it will duplicate the entry into the RA field.
Automatic Link Local Address	Here the user can select to enable or disable the Automatic Link Local Address.

Click the **Apply** button to accept the changes made for each individual section.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **View All IPv6 Address** link to view all the current IPv6 address.

Click the **View All IPv6 Address** link to see the following window.

Figure 34: IPv6 Interface Settings window

Click the **<<Back** button to return to the previous page.

Management Settings

Users can stop the scrolling of multiple pages beyond the limits of the console when using the Command Line Interface.

This window is also used to enable the DHCP auto configuration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot-up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the **Upload Log File** window description located in the **Tools** section of this manual.

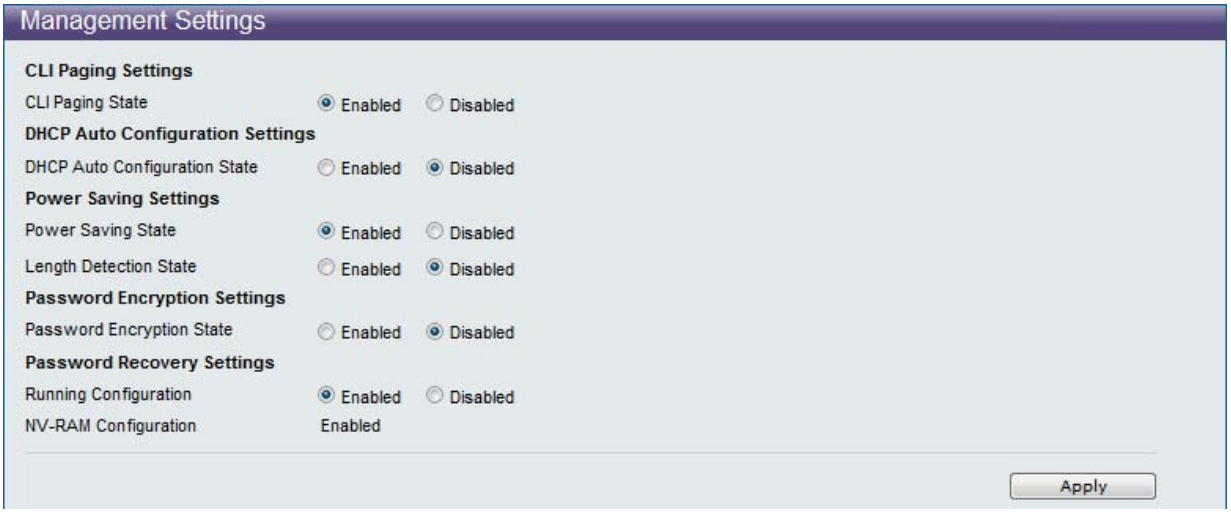
If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch's memory will be used.

This window also allows the user to implement the Switch's built-in power saving feature. When power saving is enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.

Users can also configure Password Encryption on the Switch.

To view the following window, click **Management > Management Settings**, as show below:

Figure 35: Management Settings window



The fields that can be configured are described below:

Parameter	Description
CLI Paging State	Command Line Interface paging stops each page at the end of the console. This allows you to stop the scrolling of multiple pages of text beyond the limits of the console. CLI Paging is Enabled by default. To disable it, click the Disabled radio button.
DHCP Auto Configuration State	Enable or disable the Switch's DHCP auto configuration feature. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot-up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch.
Power Saving State	Enable or disable the link down power saving mode of each physical port. The switch port will go into sleep mode when a port is not connected.
Length Detection State	Enable or disable the length detection power saving mode on the physical ports. The switch port will reduce the power feed for shorter cables.
Password Encryption State	Password encryption will encrypt the password configuration in configuration files. Password encryption is Disabled by default. To enable password encryption, click the Enabled radio button.
Running Configuration	Under the Password Recovery option, the running configuration can be enabled or disable. Being enabled, will allow the user to perform a password recovery of the running configuration.

Click the **Apply** button to accept the changes made.

Session Table

Users can display the management sessions since the Switch was last rebooted.

To view the following window, click **Management > Session Table**, as show below:

Figure 36: Session Table window

Click the **Refresh** button to refresh the display table so that new entries will appear.

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The Switch supports the SNMP versions 1, 2c, and 3. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

- **public** – Allows authorized management stations to retrieve MIB objects.
- **private** – Allows authorized management stations to retrieve and modify MIB objects.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

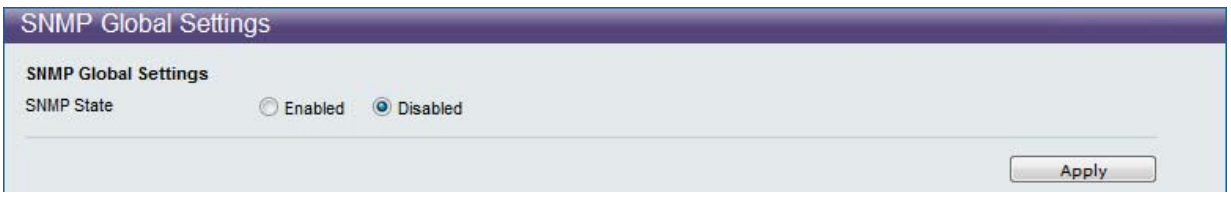
SNMP settings are configured using the menus located on the SNMP V3 folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Global Settings

SNMP global state settings can be enabled or disabled.

To view the following window, click **Management > SNMP Settings > SNMP Global Settings**, as show below:

Figure 37: SNMP Global Settings window



The fields that can be configured are described below:

Parameter	Description
SNMP State	Enable this option to use the SNMP feature.

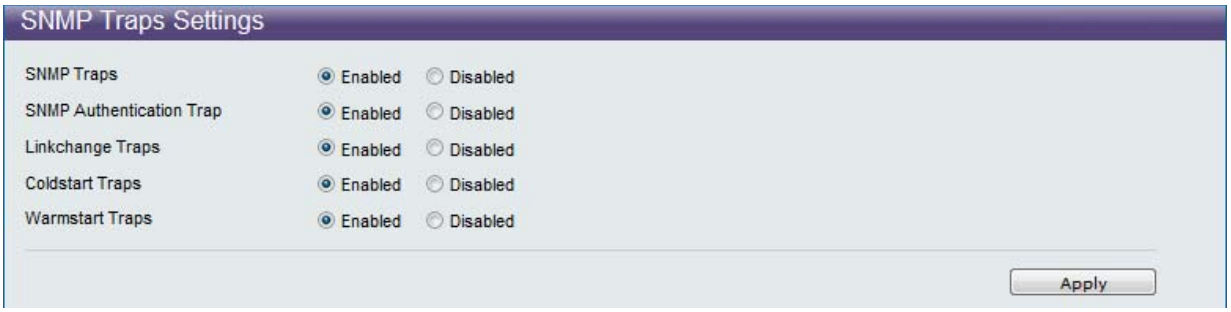
Click the **Apply** button to accept the changes made.

SNMP Traps Settings

Users can enable and disable the SNMP trap support function of the switch and SNMP authentication failure trap support, respectively.

To view the following window, click **Management > SNMP Settings > SNMP Traps Settings**, as show below:

Figure 38: SNMP Traps Settings window



The fields that can be configured are described below:

Parameter	Description
SNMP Traps	Enable this option to use the SNMP Traps feature.
SNMP Authentication Trap	Enable this option to use the SNMP Authentication Traps feature.
Linkchange Traps	Enable this option to use the SNMP Link Change Traps feature.
Coldstart Traps	Enable this option to use the SNMP Cold Start Traps feature.
Warmstart Traps	Enable this option to use the SNMP Warm Start Traps feature.

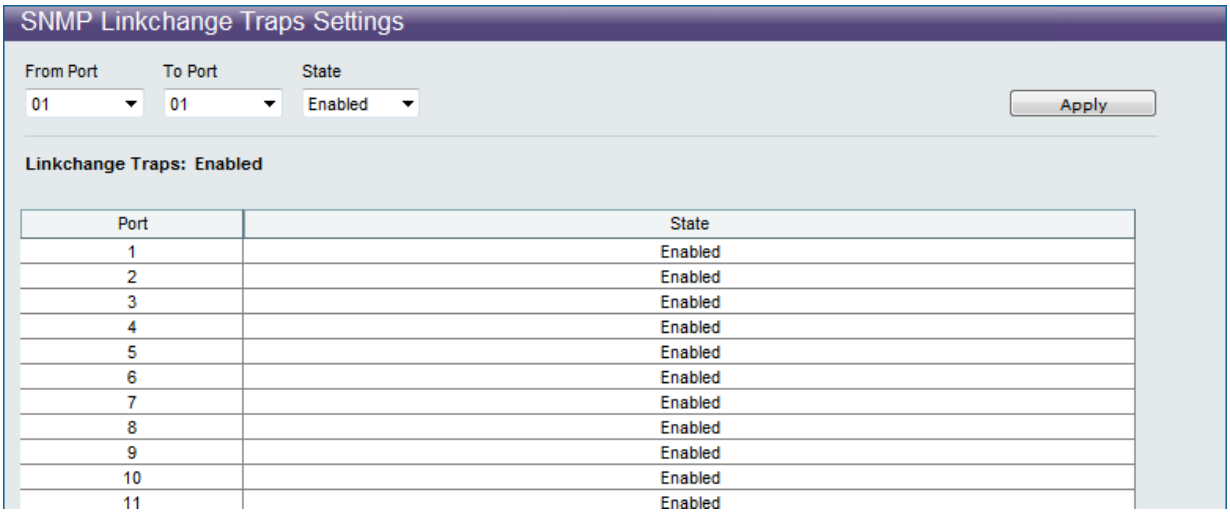
Click the **Apply** button to accept the changes made.

SNMP Linkchange Traps Settings

On this page the user can configure the SNMP link change trap settings.

To view the following window, click **Management > SNMP Settings > SNMP Linkchange Traps Settings**, as show below:

Figure 39: SNMP Linkchange Traps Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the starting and ending ports to use.
State	Use the drop-down menu to enable or disable the SNMP link change Trap.

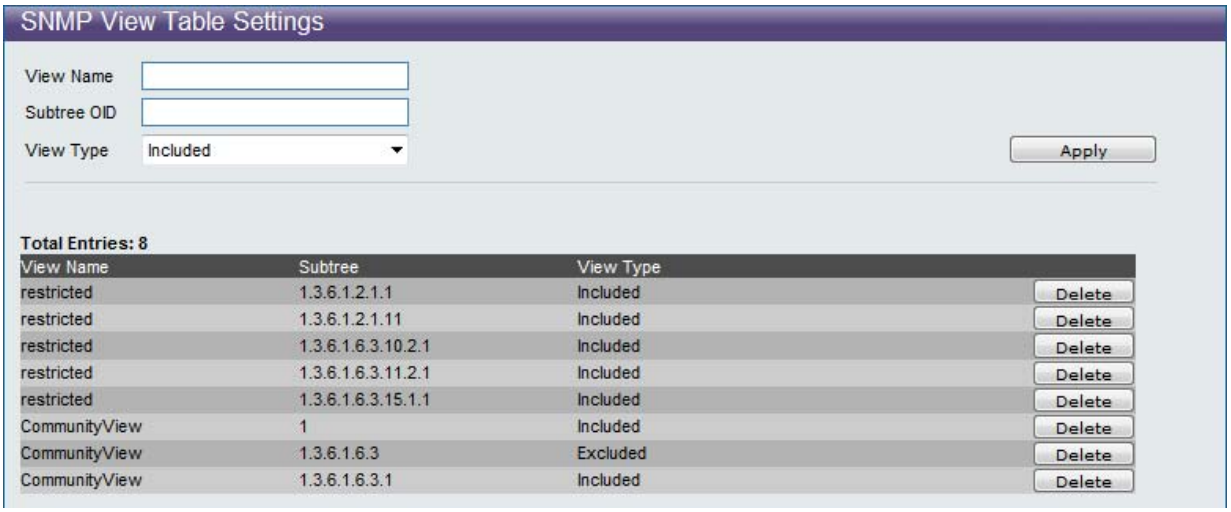
Click the **Apply** button to accept the changes made.

SNMP View Table Settings

Users can assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

To view the following window, click **Management > SNMP Settings > SNMP View Table Settings**, as show below:

Figure 40: SNMP View Table Settings window



The fields that can be configured are described below:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select Included to include this object in the list of objects that an SNMP manager can access. Select Excluded to exclude this object from the list of objects that an SNMP manager can access.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

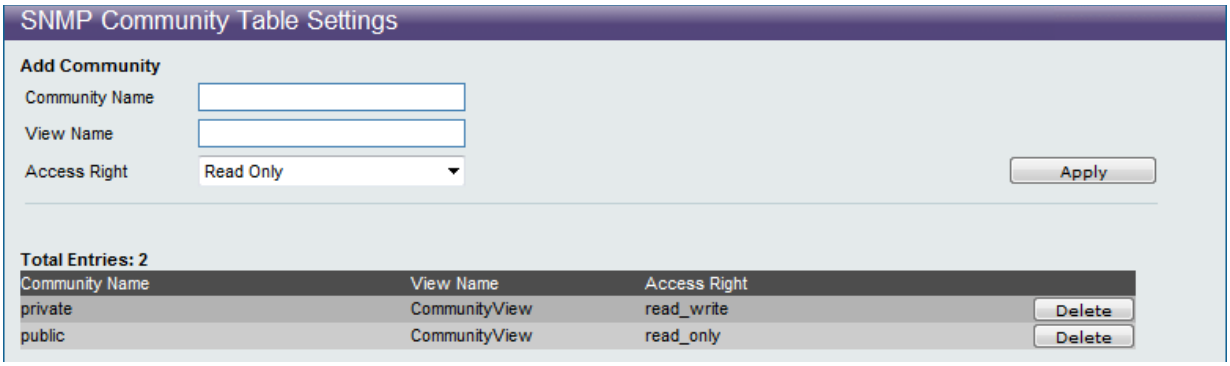
SNMP Community Table Settings

Users can create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To view the following window, click **Management > SNMP Settings > SNMP Community Table Settings**, as show below:

Figure 41: SNMP community Table Settings window



The fields that can be configured are described below:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	*Read Only* – Specify that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. *Read Write* – Specify that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

Click the **Apply** button to accept the changes made.

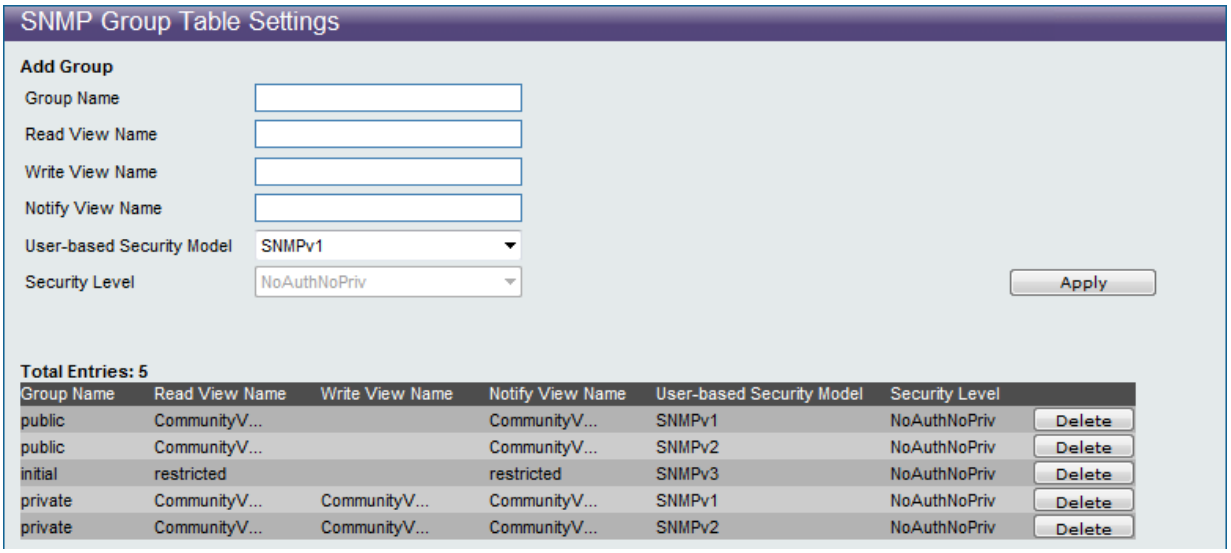
Click the **Delete** button to remove the specific entry.

SNMP Group Table Settings

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

To view the following window, click **Management > SNMP Settings > SNMP Group Table Settings**, as show below:

Figure 42: SNMP Group Table Settings window



The fields that can be configured are described below:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
User-based Security Model	*SNMPv1* – Specify that SNMP version 1 will be used. *SNMPv2* – Specify that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *SNMPv3* – Specify that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	The Security Level settings only apply to SNMPv3. *NoAuthNoPriv* – Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *AuthNoPriv* – Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *AuthPriv* – Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

Click the **Apply** button to accept the changes made.

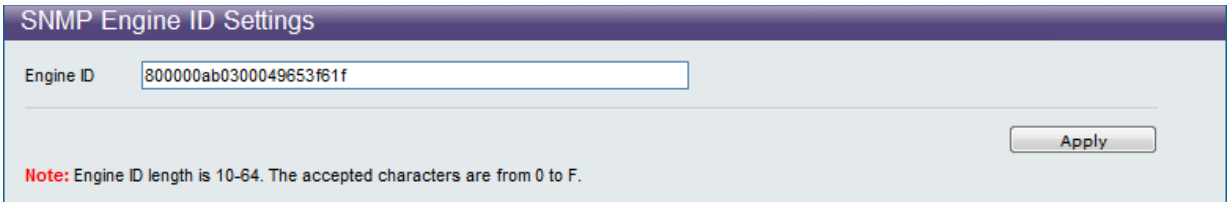
Click the **Delete** button to remove the specific entry.

SNMP Engine ID Settings

The Engine ID is a unique identifier used for SNMP V3 implementations on the Switch.

To view the following window, click **Management > SNMP Settings > SNMP Engine ID Settings**, as show below:

Figure 43: SNMP Engine ID Settings window


SNMP Engine ID Settings
Engine ID
800000ab0300049653f61f
Apply
Note: Engine ID length is 10-64. The accepted characters are from 0 to F.

The fields that can be configured are described below:

Parameter	Description
Engine ID	To change the Engine ID, type the new Engine ID value in the space provided. The SNMP engine ID displays the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by IANA (Extreme is 171). The fifth octet is 03 to indicate the rest is the MAC address of this device. The sixth to eleventh octets is the MAC address.

Click the **Apply** button to accept the changes made.

NOTE

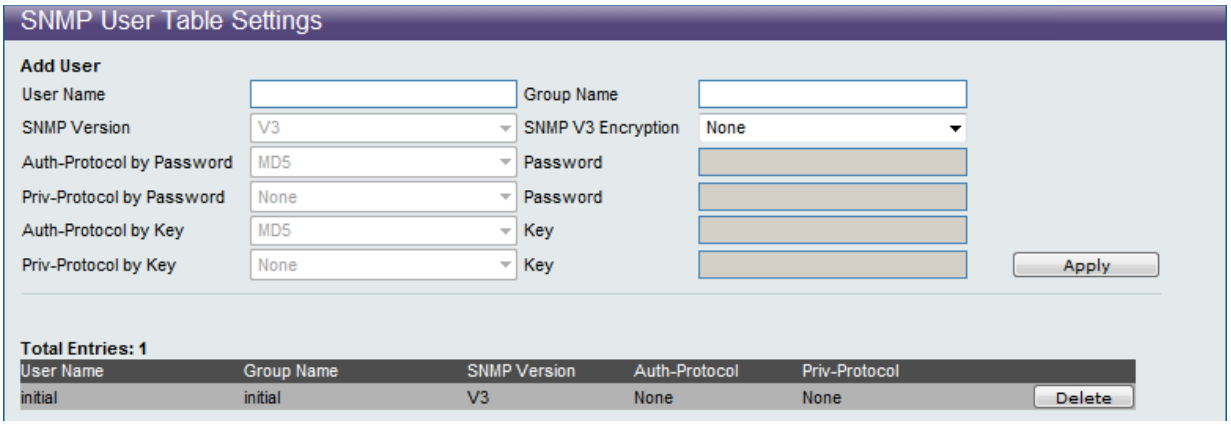
The Engine ID length is 10-64 and accepted characters can range from 0 to F.

SNMP User Table Settings

This window displays all of the SNMP User's currently configured on the Switch.

To view the following window, click **Management > SNMP Settings > SNMP User Table Settings**, as show below:

Figure 44: SNMP User Table Settings window



The fields that can be configured are described below:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V3* – Indicates that SNMP version 3 is in use.
SNMP V3 Encryption	Use the drop-down menu to enable encryption for SNMP V3. This is only operable in SNMP V3 mode. The choices are *None*, *Password*, or *Key*.
Auth-Protocol	*MD5* – Specify that the HMAC-MD5-96 authentication level will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password. *SHA* – Specify that the HMAC-SHA authentication protocol will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.
Priv-Protocol	*None* – Specify that no authorization protocol is in use. *DES* – Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.

Click the **Apply** button to accept the changes made.

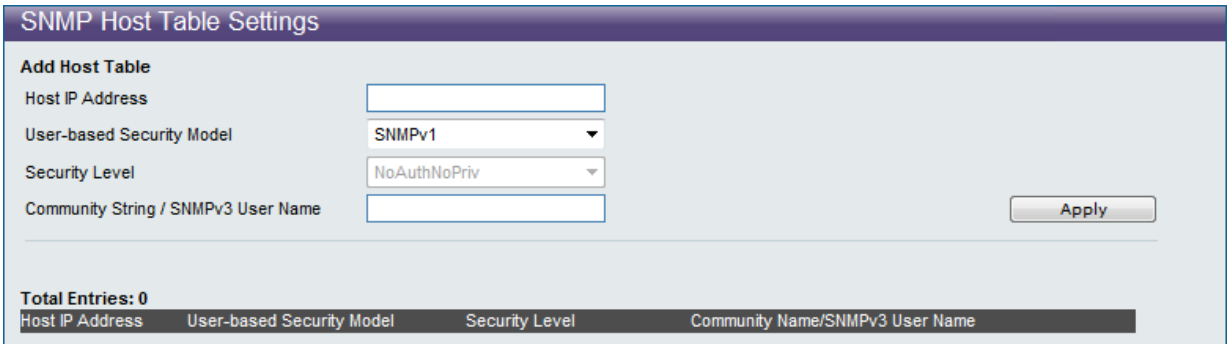
Click the **Delete** button to remove the specific entry.

SNMP Host Table Settings

Users can set up SNMP trap recipients for IPv4.

To view the following window, click **Management > SNMP Settings > SNMP Host Table Settings**, as show below:

Figure 45: SNMP Host Table Settings window



The fields that can be configured are described below:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* – Specify that SNMP version 1 will be used.
	SNMPv2 – Specify that SNMP version 2 will be used.
	SNMPv3 – Specify that SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.
	AuthNoPriv – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.
	AuthPriv – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String / SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

Click the **Apply** button to accept the changes made.

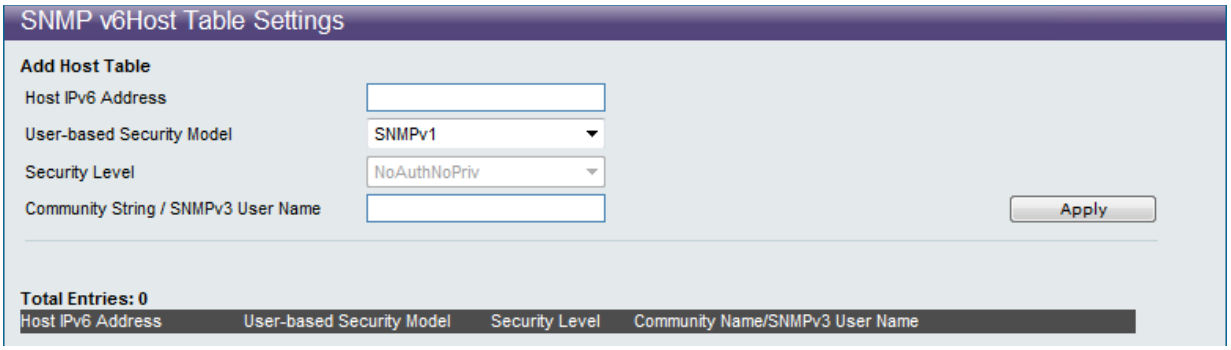
Click the **Delete** button to remove the specific entry.

SNMPv6 Host Table Settings

Users can set up SNMP trap recipients for IPv6.

To view the following window, click **Management > SNMP Settings > SNMPv6 Host Table Settings**, as show below:

Figure 46: SNMPv6 Host Table Settings



The fields that can be configured are described below:

Parameter	Description
Host IPv6 Address	Type the IPv6 address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* – Specifies that SNMP version 1 will be used.
	SNMPv2 – Specifies that SNMP version 2 will be used.
	SNMPv3 – Specifies that SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.
	AuthNoPriv – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.
	AuthPriv – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String / SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

Click the **Apply** button to accept the changes made.

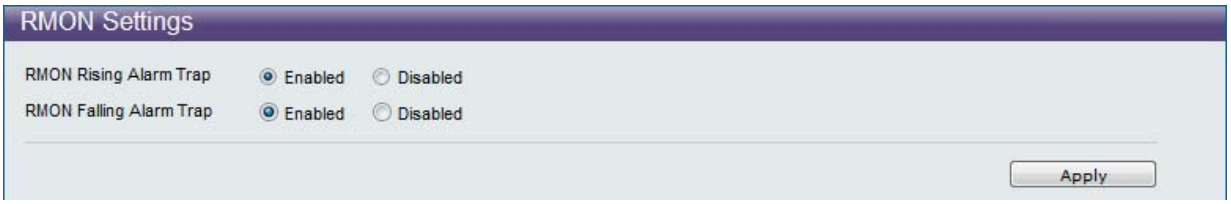
Click the **Delete** button to remove the specific entry.

RMON Settings

On this page the user can enable or disable remote monitoring (RMON) for the rising and falling alarm trap feature for the SNMP function on the Switch.

To view the following window, click **Management > SNMP Settings > RMON Settings**, as show below:

Figure 47: RMON Settings window



The fields that can be configured are described below:

Parameter	Description
RMON Rising Alarm Trap	Enable this option to use the RMON Rising Alarm Trap Feature.
RMON Falling Alarm Trap	Enable this option to use the RMON Falling Alarm Trap Feature.

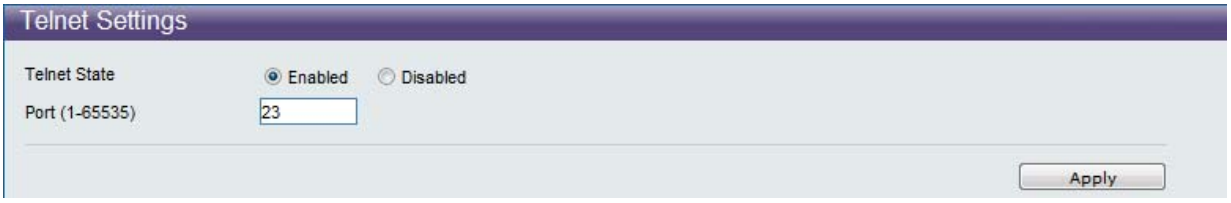
Click the **Apply** button to accept the changes made.

Telnet Settings

Users can configure Telnet Settings on the Switch.

To view the following window, click **Management > Telnet Settings**, as show below:

Figure 48: Telnet Settings window



The fields that can be configured are described below:

Parameter	Description
Telnet State	Telnet configuration is Enabled by default. If you do not want to allow configuration of the system through Telnet choose Disabled.
Port (1-65535)	The TCP port number used for Telnet management of the Switch. The “well-known” TCP port for the Telnet protocol is *23*.

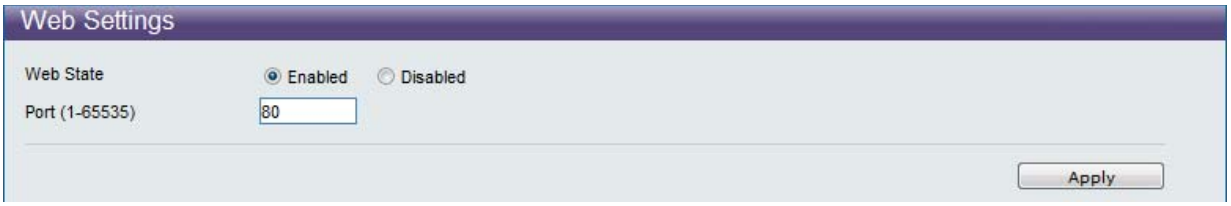
Click the **Apply** button to accept the changes made.

Web Settings

Users can configure the Web settings on the Switch.

To view the following window, click **Management > Web Settings**, as show below:

Figure 49: Web Settings window



The fields that can be configured are described below:

Parameter	Description
Web Status	Web-based management is Enabled by default. If you choose to disable this by clicking Disabled, you will lose the ability to configure the system through the web interface as soon as these settings are applied.
Port (1-65535)	The TCP port number used for web-based management of the Switch. The "well-known" TCP port for the Web protocol is *80*.

Click the **Apply** button to accept the changes made.

4 L2 Features

CHAPTER

VLAN

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an

autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes about VLANs on the Switch

- No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.
- The Switch supports IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
- The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
- The "default" VLAN has a VID = 1.
- The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** – A port on a switch where packets are flowing into the Switch and VLAN decisions must be made.
- **Egress port** – A port on a switch where packets are flowing out of the Switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

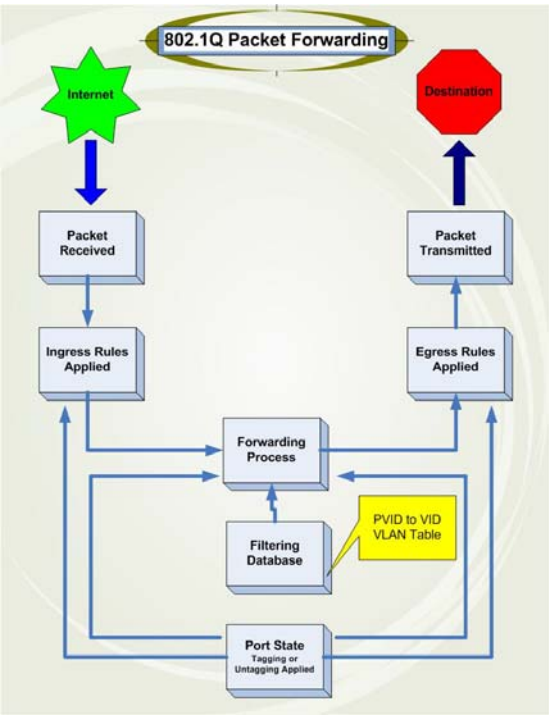
Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding
- Packet forwarding decisions are made based upon the following three types of rules:
- Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.
- Forwarding rules between ports – decides whether to filter or forward the packet.
- Egress rules – determines if the packet must be sent tagged or untagged.

Figure 50: IEEE 802.1Q Packet Forwarding

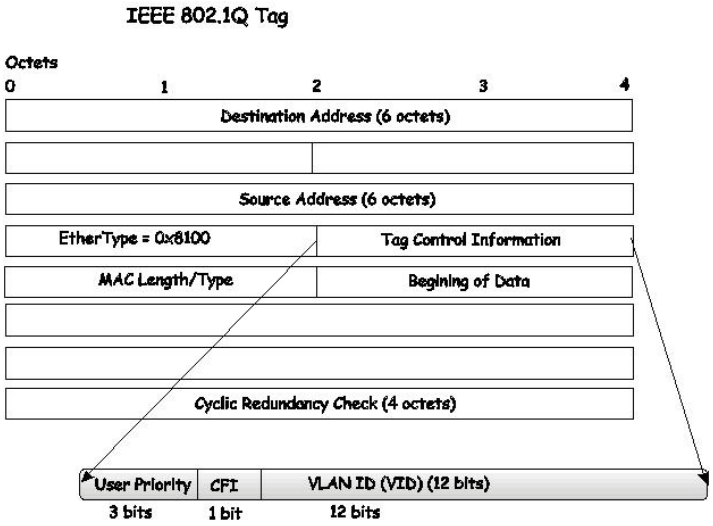


802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

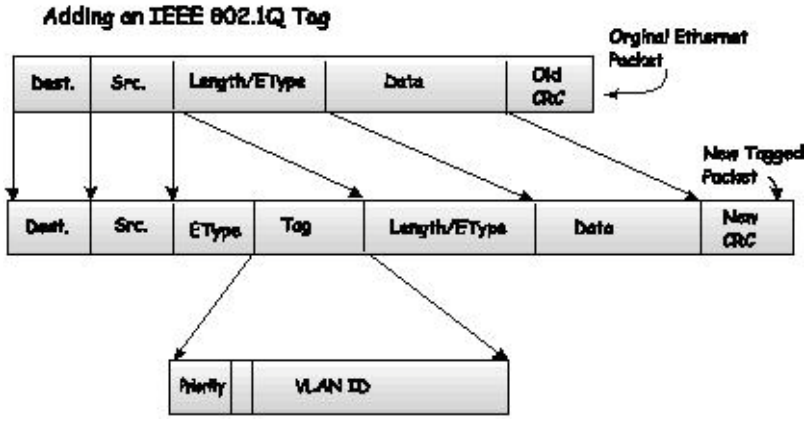
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

Figure 51: IEEE 802.1Q Tag



The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Figure 52: Adding an IEEE 802.1Q Tag



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it.

If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a

member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

NOTE

If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7
Engineering	2	9, 10
Sales	5	1, 2, 3, 4

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

VLAN Segmentation

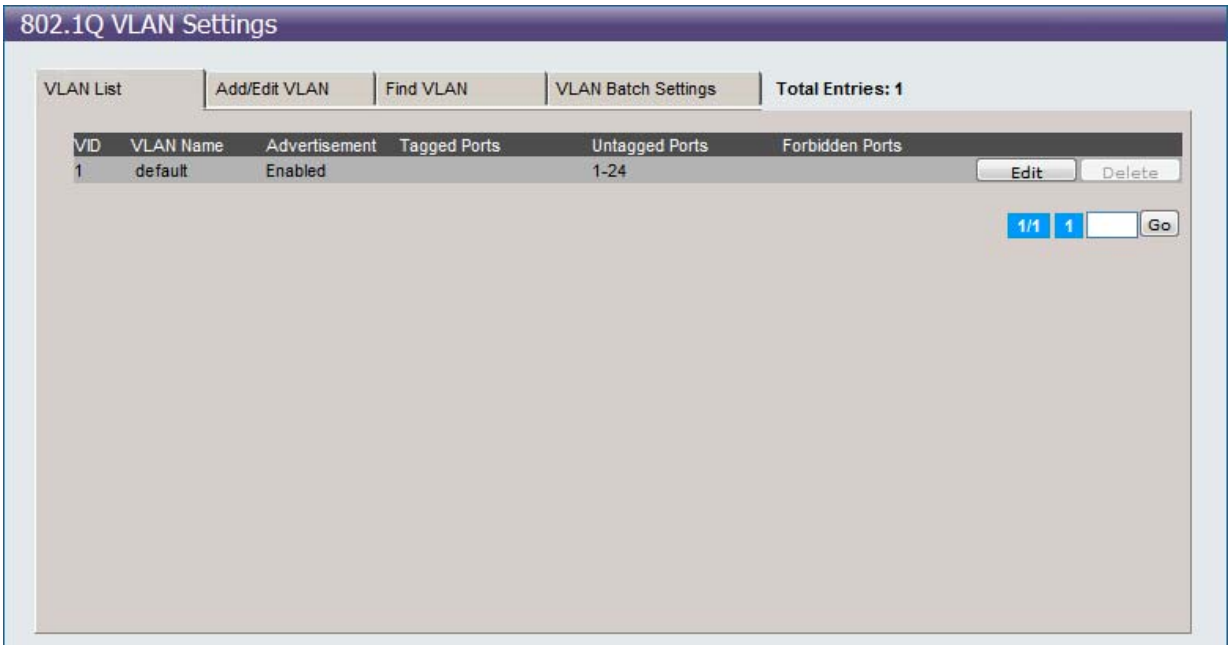
Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

802.1Q VLAN Settings

The **VLAN List** tab lists all previously configured VLANs by VLAN ID and VLAN Name.

To view the following window, click **L2 Features > VLAN > 802.1Q VLAN Settings**, as show below:

Figure 53: 802.1Q VLAN Settings –VLAN List Tab window



Click the **Edit** button to re-configure the specific entry.

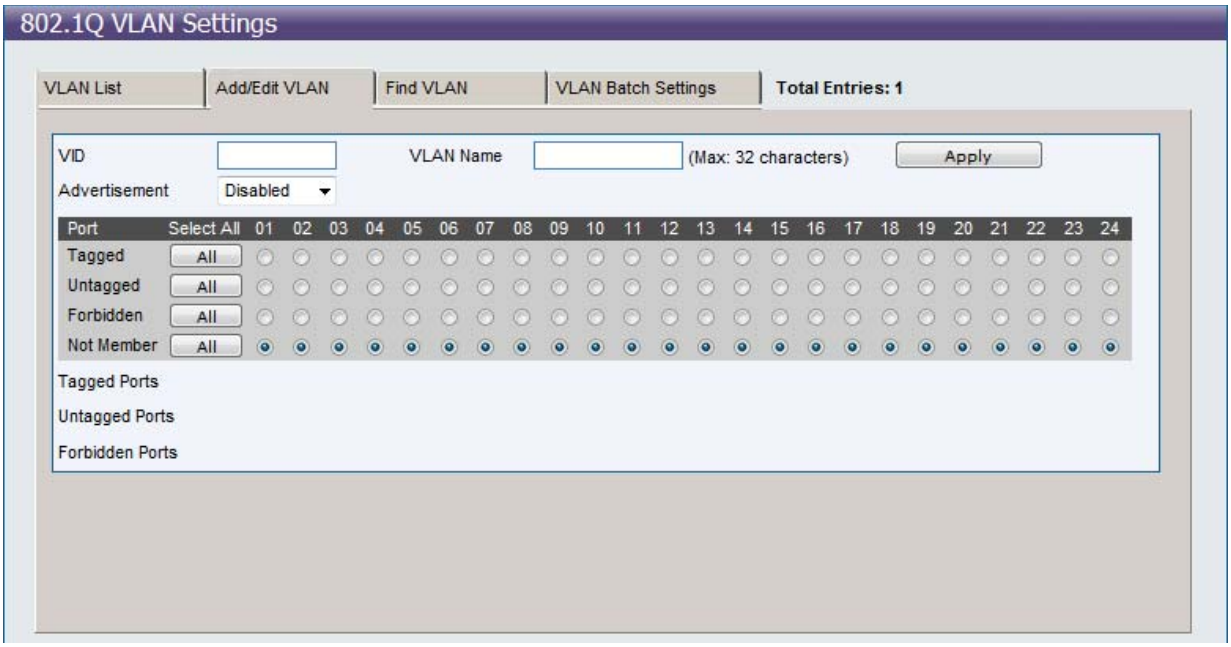
Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To create a new 802.1Q VLAN or modify an existing 802.1Q VLAN, click the **Add/Edit VLAN** tab.

A new tab will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN.

Figure 54: 802.1Q VLAN Settings – Add/Edit VLAN Tab window



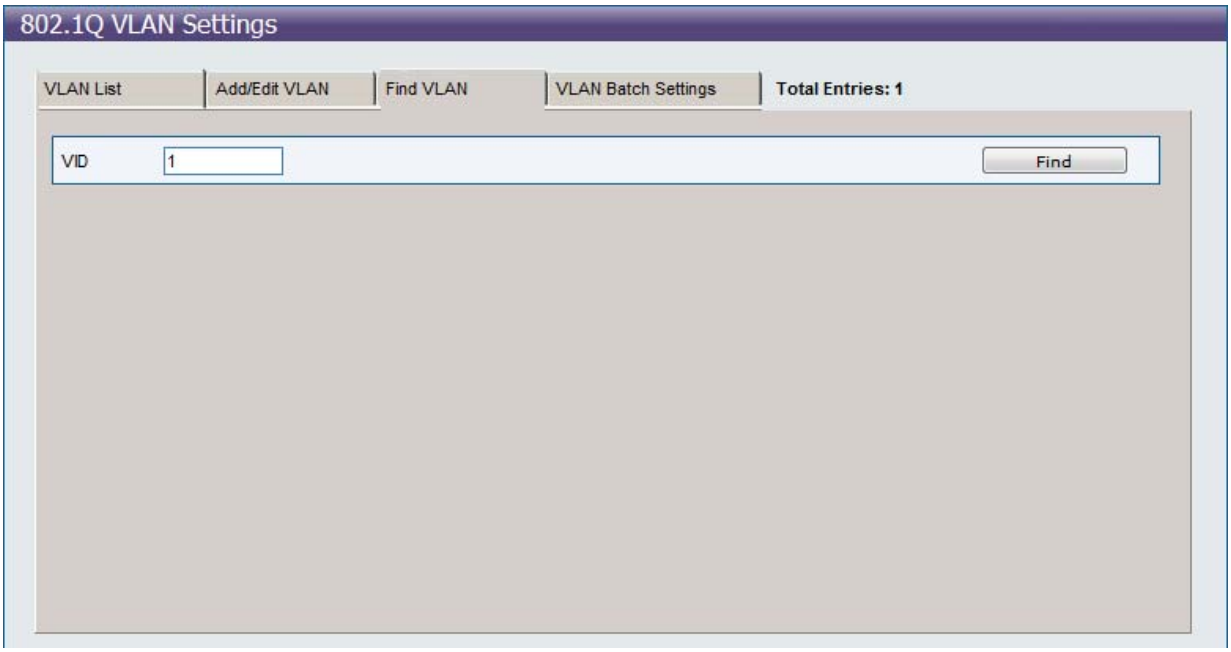
The fields that can be configured are described below:

Parameter	Description
VID	Allow the entry of a VLAN ID or displays the VLAN ID of an existing VLAN in the **Add/Edit VLAN** tab. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allow the entry of a name for the new VLAN or for editing the VLAN name in the **Add/Edit VLAN** tab.
Advertisement	Enable this function to allow the Switch sending out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port	Display all ports of the Switch for the configuration option.
Tagged	Specify the port as 802.1Q tagging. Clicking the radio button will designate the port as tagged. Click the **All** button to select all ports.
Untagged	Specify the port as 802.1Q untagged. Clicking the radio button will designate the port as untagged. Click the **All** button to select all ports.
Forbidden	Click the radio button to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. Click the **All** button to select all ports.
Not Member	Click the radio button to allow an individual port to be specified as a non-VLAN member. Click the **All** button to select all ports.

Click the **Apply** button to accept the changes made.

To search for a VLAN, click the **Find VLAN** tab. A new tab will appear, as shown below.

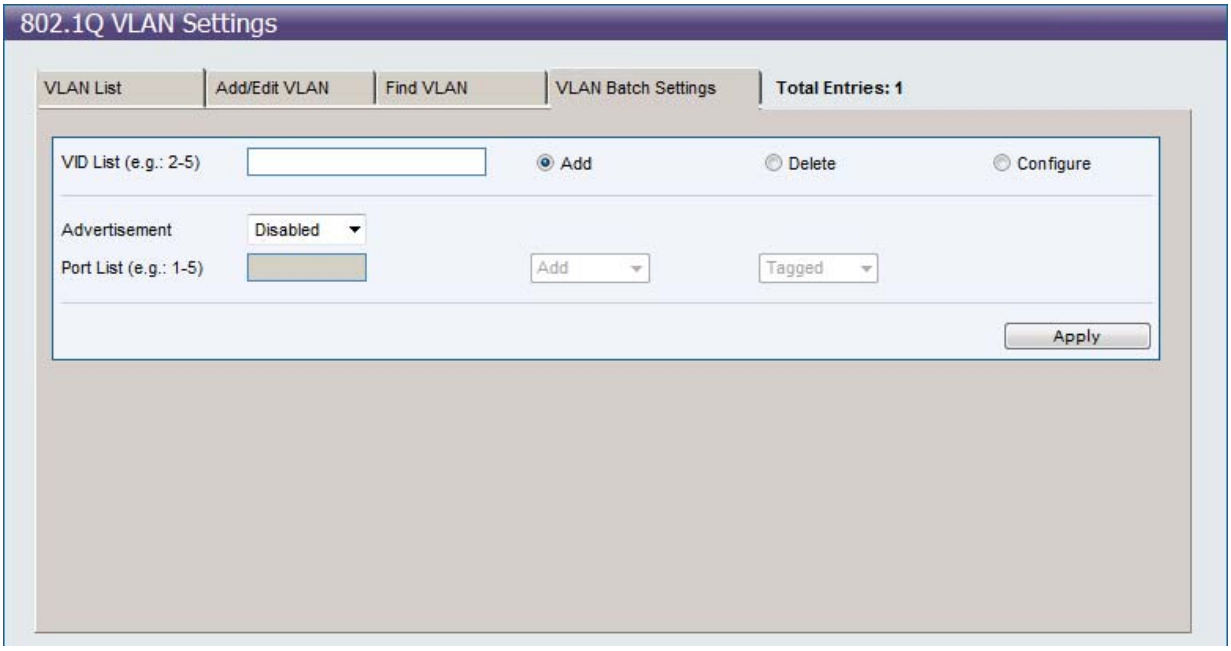
Figure 55: 802.1Q VLAN Settings – Find VLAN Tab window



Enter the VLAN ID number in the field offered and then click the **Find** button. You will be redirected to the **VLAN List** tab.

To create, delete and configure a VLAN Batch entry click the **VLAN Batch Settings** tab, as shown below.

Figure 56: 802.1Q VLAN Settings – VLAN Batch Settings Tab window



The fields that can be configured are described below:

Parameter	Description

Parameter	Description
VID List	Enter a VLAN ID List that can be added, deleted or configured.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port List	Allows an individual port list to be added or deleted as a member of the VLAN.
Tagged	Specify the port as 802.1Q tagged. Use the drop-down menu to designate the port as tagged.
Untagged	Specify the port as 802.1Q untagged. Use the drop-down menu to designate the port as untagged.
Forbidden	Specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. Use the drop-down menu to designate the port as forbidden.

Click the **Apply** button to accept the changes made.

NOTE

The Switch supports up to 4k static VLAN entries.

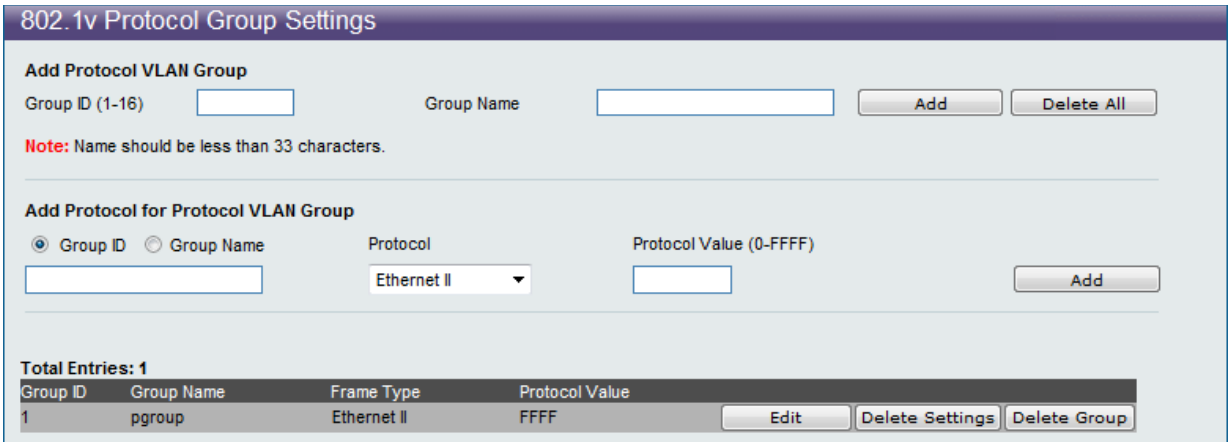
802.1v Protocol VLAN

802.1v Protocol Group Settings

The user can create Protocol VLAN groups and add protocols to that group. The 802.1v Protocol VLAN Group Settings support multiple VLANs for each protocol and allows the user to configure the untagged ports of different protocols on the same physical port. For example, it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port. The lower half of the table displays any previously created groups.

To view the following window, click **L2 Features > VLAN > 802.1v protocol VLAN > 802.1v Protocol Group Settings**, as show below:

Figure 57: 802.1v Protocol Group Settings window



The fields that can be configured are described below:

Parameter	Description

Parameter	Description
Group ID	Select an ID number for the group, between *1* and *16*.
Group Name	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 32 characters.
Protocol	This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Use the drop-down menu to toggle between *Ethernet II*, *IEEE802.3 SNAP*, and *IEEE802.3 LLC*.
Protocol Value	Enter a value for the Group. The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is a 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete Settings** button to remove the Protocol for the Protocol VLAN Group information for the specific entry.

Click the **Delete Group** button to remove the entry completely.

NOTE

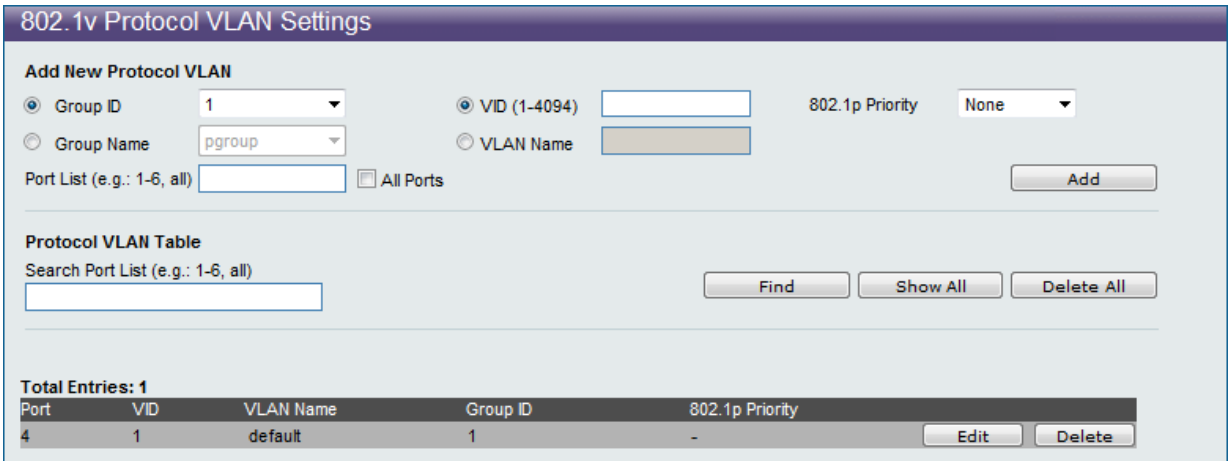
The Group name value should be less than 33 characters

802.1v Protocol VLAN Settings

The user can configure Protocol VLAN settings. The lower half of the table displays any previously created settings.

To view the following window, click **L2 Features > VLAN > 802.1v protocol VLAN > 802.1v Protocol VLAN Settings**, as show below:

Figure 58: 802.1v Protocol VLAN Settings window



The fields that can be configured are described below:

Parameter	Description
Group ID	Select a previously configured Group ID from the drop-down menu.
Group Name	Select a previously configured Group Name from the drop-down menu.
VID (1-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to create.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to create.
802.1p Priority	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. Click the corresponding box if you want to set the 802.1p default priority of a packet to the value entered in the Priority (0-7) field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.

Parameter	Description
Port List	Select the specified ports you wish to configure by entering the port number in this field, or tick the **All Ports** check box.
Search Port List	This function allows the user to search all previously configured port list settings and display them on the lower half of the table. To search for a port list enter the port number you wish to view and click **Find**. To display all previously configured port lists on the bottom half of the screen click the **Show All** button, to clear all previously configured lists click the **Delete All** button.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the Protocol VLANs configured.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

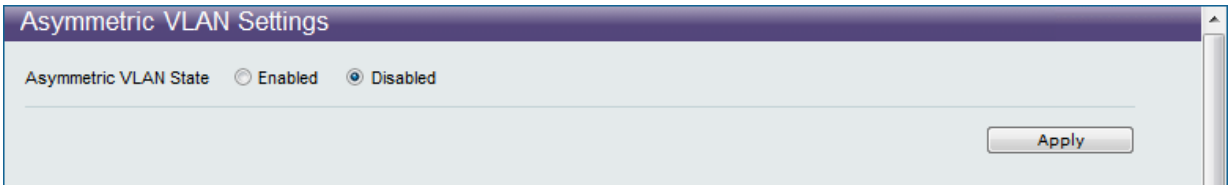
Click the **Delete** button to remove the specific entry.

Asymmetric VLAN Settings

Shared VLAN Learning is a primary example of the requirement for Asymmetric VLANs. Under normal circumstances, a pair of devices communicating in a VLAN environment will both send and receive using the same VLAN; however, there are some circumstances in which it is convenient to make use of two distinct VLANs, one used for A to transmit to B and the other used for B to transmit to A in these cases Asymmetric VLANs are needed. An example of when this type of configuration might be required, would be if the client was on a distinct IP subnet, or if there was some confidentiality-related need to segregate traffic between the clients.

To view this window click **L2 Features > VLAN > Asymmetric VLAN Settings**, as show below:

Figure 59: Asymmetric VLAN Settings window



Click **Apply** to implement changes.

GVRP

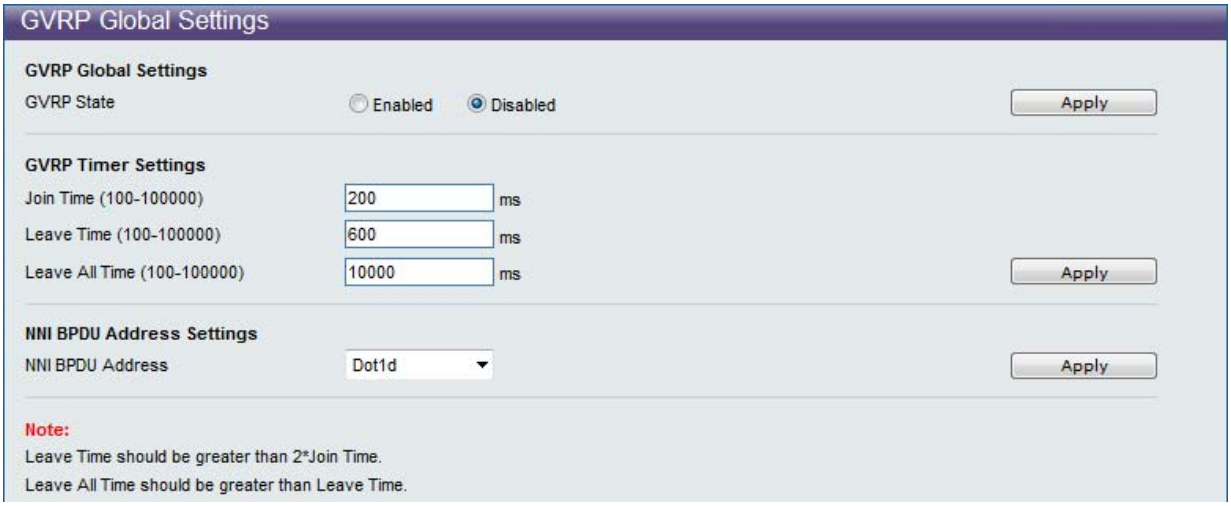
GVRP Global Settings

Users can determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used

to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings.

To view the following window, click **L2 Features > VLAN > GVRP > GVRP Global Settings**, as show below:

Figure 60: GVRP Global Settings window



The fields that can be configured are described below:

Parameter	Description

Parameter	Description
GVRP State	Click the radio buttons to enable or disable the GVRP State.
Join Time	Enter the Join Time value in milliseconds.
Leave Time	Enter the Leave Time value in milliseconds.
Leave All Time	Enter the Leave All Time value in milliseconds.
NNI BPDU Address	Used to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.

Click the **Apply** button to accept the changes made for each individual section.

NOTE

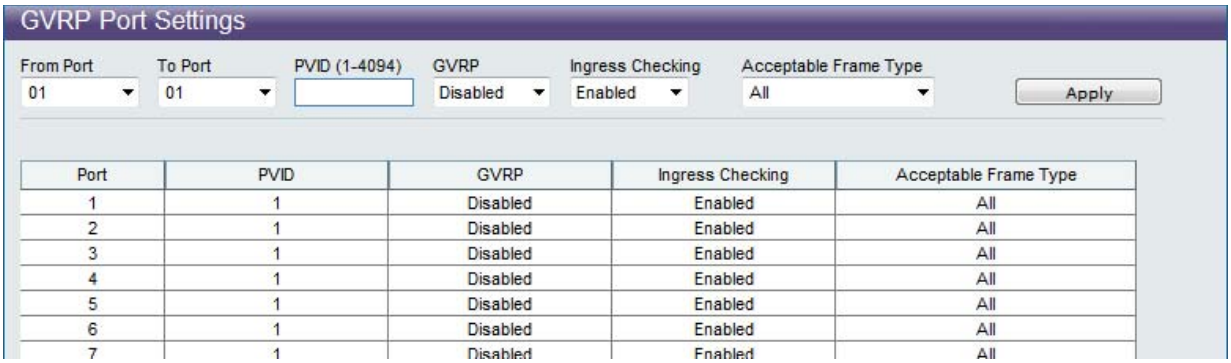
The **Leave Time** value should be greater than twice the **Join Time** value. The **Leave All Time** value should be greater than the **Leave Time** value.

GVRP Port Settings

On this page the user can configure the GVRP port parameters.

To view the following window, click **L2 Features > VLAN > GVRP > GVRP Port Settings**, as show below:

Figure 61: GVRP Port Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the starting and ending ports to use.
PVID	This field is used to manually assign a PVID to a VLAN. The Switch's default is to assign all ports to the default VLAN with a VID of 1.The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is *Enabled*, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The GARP VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.
Ingress Checking	This drop-down menu allows the user to enable the port to compare the VID tag of an incoming packet with the port VLAN membership. If enable ingress checking and the reception port is not the member port of the frame's VLAN, the frame shall be discarded.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *All*, which mean both tagged and untagged frames will be accepted. *All* is enabled by default.

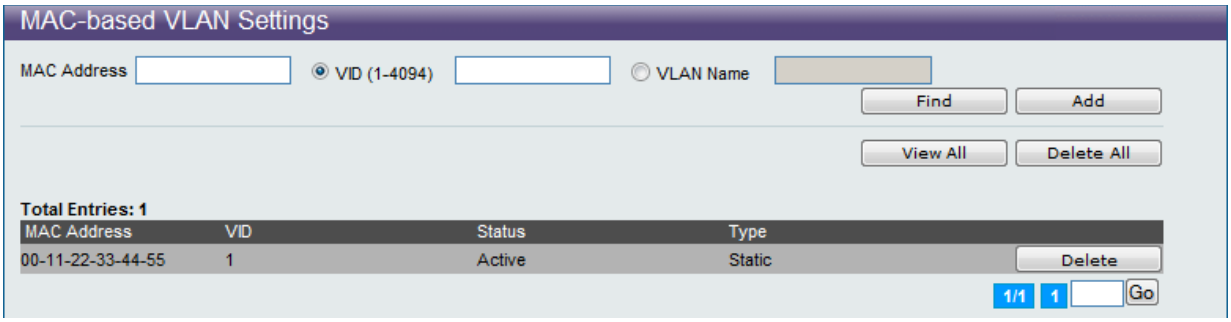
Click the **Apply** button to accept the changes made.

MAC-based VLAN Settings

Users can create new MAC-based VLAN entries, search and delete existing entries. When a static MAC-based VLAN entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the authentication function operating on this port.

To view the following window, click **L2 Features > VLAN > MAC-based VLAN Settings**, as show below:

Figure 62: MAC-based VLAN Settings



The fields that can be configured are described below:

Parameter	Description
MAC Address	Specify the MAC address to be re-authenticated by entering it into the MAC Address field.
VID	Select this option and enter the VLAN ID.
VLAN Name	Select this option and enter the VLAN name of a previously configured VLAN.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

Private VLAN Settings

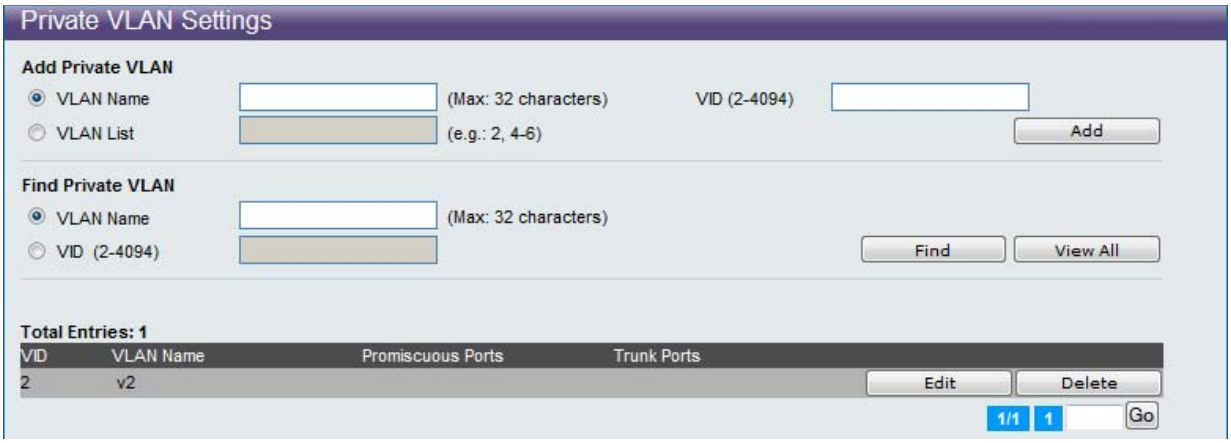
A private VLAN is comprised of a primary VLAN, up to one isolated VLAN, and a number of community VLANs. A private VLAN ID is presented by the VLAN ID of the primary VLAN. The command used to associate or de-associate a secondary VLAN with a primary VLAN.

A secondary VLAN cannot be associated with multiple primary VLANs. The untagged member port of the primary VLAN is named as the promiscuous port. The tagged member port of the primary VLAN is named as the trunk port. A promiscuous port of a private VLAN cannot be promiscuous port of other private VLANs. The primary VLAN member port cannot be a secondary VLAN member at the same time, or vice versa. A secondary VLAN can only have the untagged member port. The member port of a secondary VLAN cannot be member port of other secondary VLAN at the same time. When a VLAN is associated with a primary VLAN as the secondary VLAN, the promiscuous port of the primary VLAN will behave as the untagged member of the secondary VLAN, and the trunk port of the primary VLAN will behave as the tagged member of the secondary VLAN. A secondary VLAN cannot be specified with advertisement. Only the primary VLAN can be configured as a layer 3 interface. The private VLAN member port cannot be configured with the traffic segmentation function.

This window allows the user to configure the private VLAN parameters.

To view the following window, click **L2 Features > VLAN > Private VLAN Settings**, as show below:

Figure 63: Private VLAN Settings window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter a VLAN name.
VID (2-4094)	Enter a VID value.
VLAN List	Enter a list of VLAN ID.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Edit** button to configure the secondary VLAN.

Click the **Delete** button to remove the specific entry.

Click the **Edit** button to see the following window.

Figure 64: Private VLAN Settings - Edit window

The fields that can be configured are described below:

Parameter	Description
Secondary VLAN Type	Use the drop-down menu to select secondary VLAN type between *Isolated* or *Community*.
Secondary VLAN Name	Enter a secondary VLAN name.
Secondary VLAN List	Enter a list of secondary VLAN ID.

Click the **Add** button to add a new entry based on the information entered.

Click the **View Private VLAN List** link to view all the private VLAN.

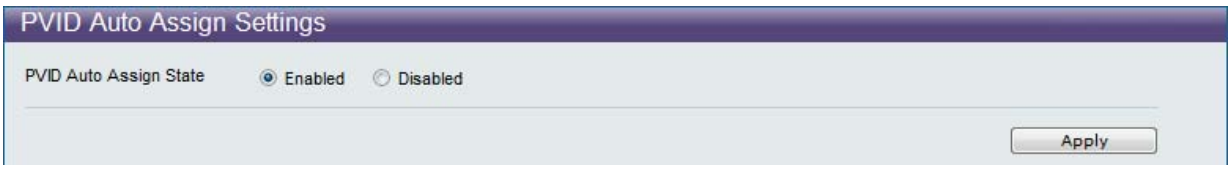
Click the **Delete** to remove the specified entry.

PVID Auto Assign Settings

Users can enable or disable PVID Auto Assign Status. The default setting is enabled.

To view the following window, click **L2 Features > VLAN > PVID Auto Assign Settings**, as show below:

Figure 65: PVID Auto Assign Settings window



Click the **Apply** button to accept the changes made.

Voice VLAN

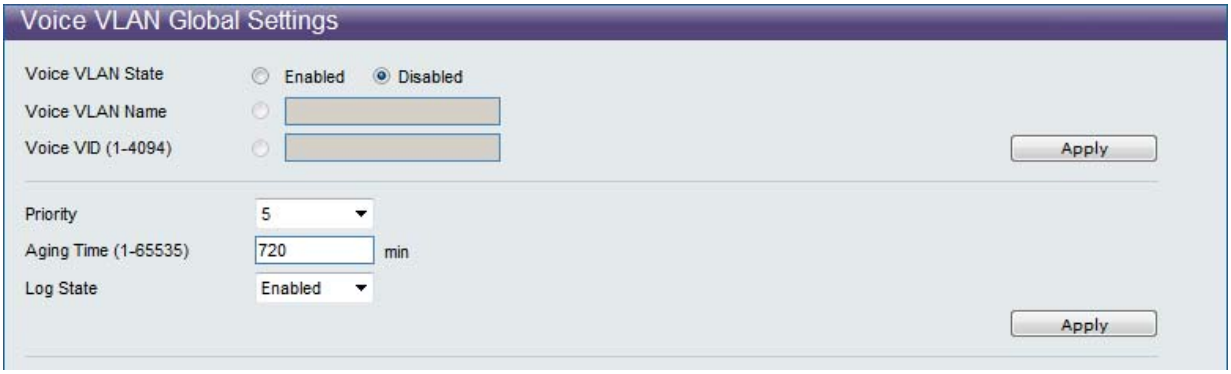
Voice VLAN Global Settings

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global Settings**, as show below:

Figure 66: Voice VLAN Global Settings window



The fields that can be configured are described below:

Parameter	Description
Voice VLAN State	The state of the voice VLAN.
Voice VLAN Name	The name of the voice VLAN.
Voice VID	The VLAN ID of the voice VLAN.
Priority	The priority of the voice VLAN, the range is 0 – 7. The default priority is 5.
Aging Time	The aging time to set, the range is 1 – 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.
Log State	Used to enable/disable sending of issue of voice VLAN log.

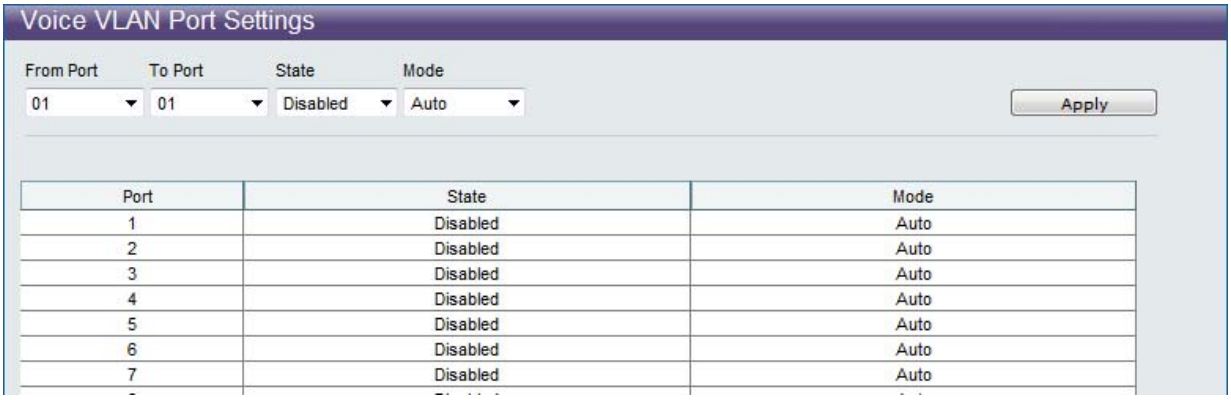
Click the **Apply** button to accept the changes made for each individual section.

Voice VLAN Port Settings

This page is used to show the ports voice VLAN information.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Port Settings**, as show below:

Figure 67: Voice VLAN Port Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Here the user can select a range of port to display.
State	Here the user can configure the state of the port.
Mode	Here the user can configure the mode of the port.

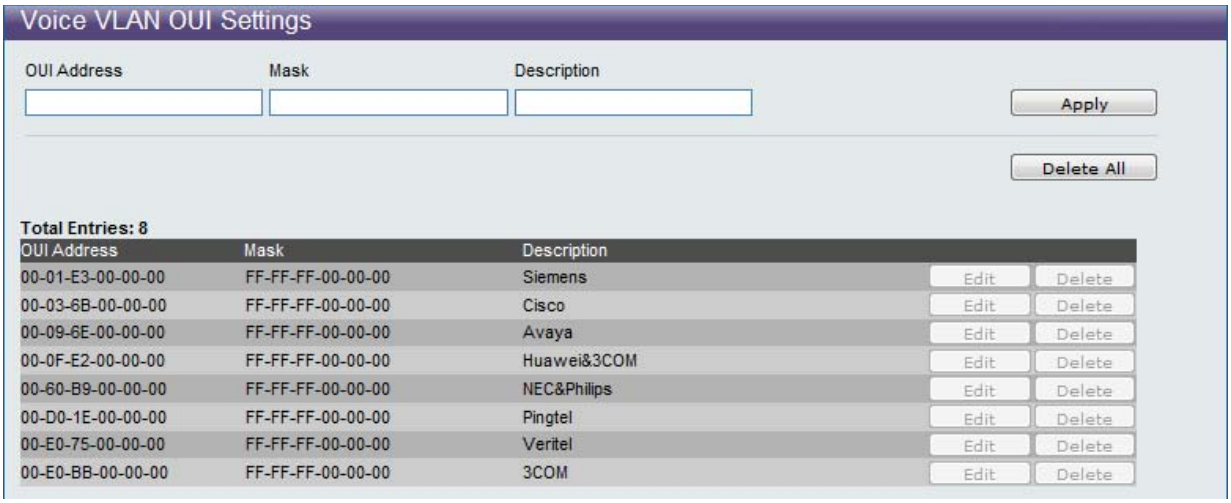
Click the **Apply** button to accept the changes made.

Voice VLAN OUI Settings

This page is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI** Settings, as show below:

Figure 68: Voice VLAN OUI Settings window



The fields that can be configured are described below:

Parameter	Description
OUI Address	User defined OUI MAC address.
Mask	User defined OUI MAC address mask.
Description	The description for the user defined OUI.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

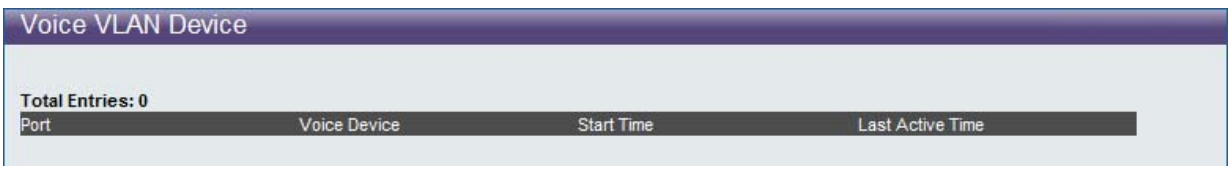
Click the **Delete** button to remove the specific entry.

Voice VLAN Device

This page is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port, the activate time is the latest time saw the device sending the traffic.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Device**, as show below:

Figure 69: Voice VLAN Device window



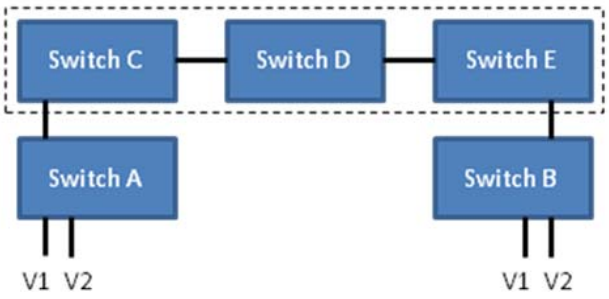
VLAN Trunk Settings

Enable VLAN on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without a VLAN Trunk, you must first configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with VLAN Trunk enabled on a port(s) in each intermediary switch, you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

Refer to the following figure for an illustrated example.

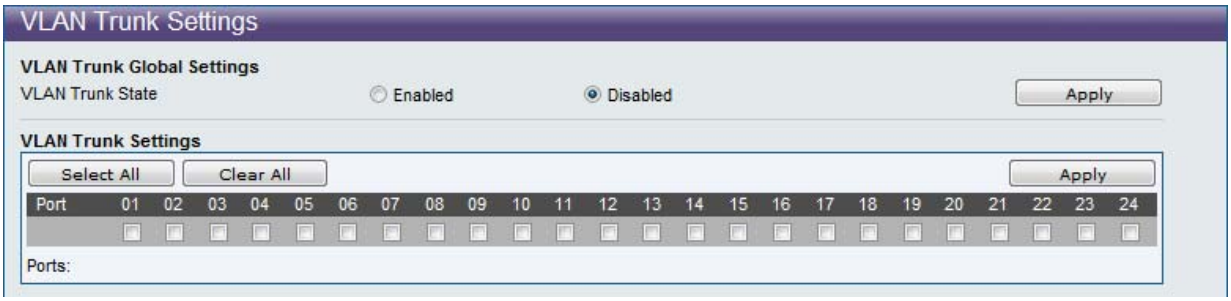
Figure 70: Example of VLAN Trunk



Users can combine a number of VLAN ports together to create VLAN trunks.

To view the following window, click **L2 Features > VLAN > VLAN Trunk Settings**, as show below:

Figure 71: VLAN Trunk Settings window



The fields that can be configured are described below:

Parameter	Description
VLAN Trunk State	Enable or disable the VLAN trunking global state.
Ports	The ports to be configured. By clicking the **Select All** button, all the ports will be included. By clicking the **Clear All** button, all the ports will not be included.

Click the **Apply** button to accept the changes made for each individual section.

Browse VLAN

Users can display the VLAN status for each of the Switch's ports viewed by VLAN. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button.

To view the following window, click **L2 Features > VLAN > Browse VLAN**, as show below:

Figure 72: Browse VLAN window

Browse VLAN
VID
Find
VID: 1
VLAN Name: default
VLAN Type: Static
Advertisement: Enabled
Total Entries: 3
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
U U U U U U U U U U U U U U U U U U U U U U U U
1/3 1 2 3 > >> Go
Note: T: Tagged Port, U: Untagged Port, F: Forbidden Port

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

NOTE

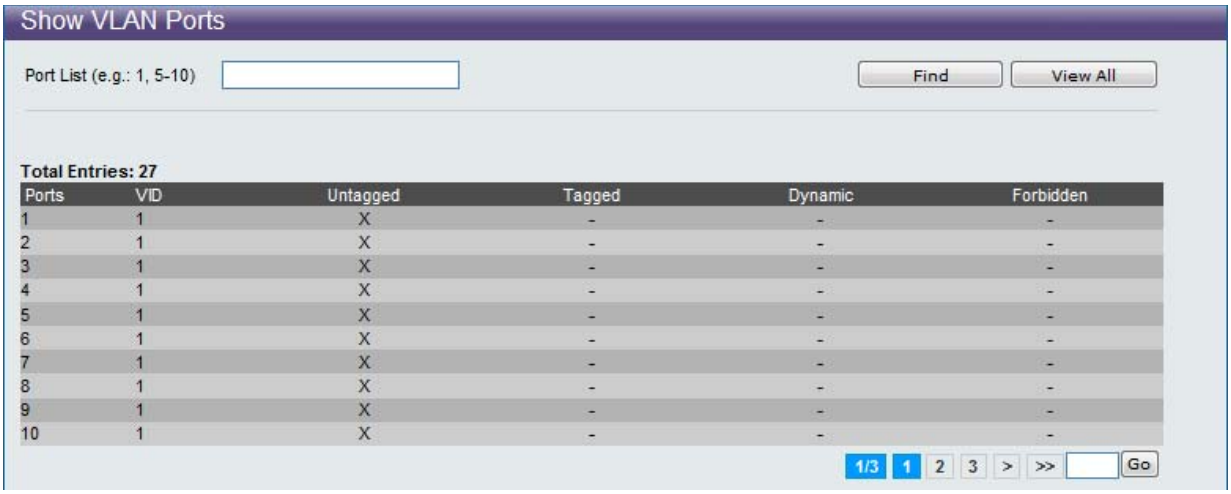
The abbreviations used on this page are **Tagged Port (T)**, **Untagged Port (U)** and **Forbidden Port (F)**.

Show VLAN Ports

Users can display the VLAN ports of the Switch's viewed by VID. Enter a Port or a **Port List** in the field at the top of the window and click the **Find** button.

To view the following window, click **L2 Features > VLAN > Show VLAN Ports**, as show below:

Figure 73: Show VLAN Ports window


Show VLAN Ports
Port List (e.g.: 1, 5-10)
Find
View All
Total Entries: 27
Ports VID Untagged Tagged Dynamic Forbidden
1 1 X - - -
2 1 X - - -
3 1 X - - -
4 1 X - - -
5 1 X - - -
6 1 X - - -
7 1 X - - -
8 1 X - - -
9 1 X - - -
10 1 X - - -
1/3 1 2 3 > >> Go

Click the **View All** button to display all the existing entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

QinQ

Double or Q-in-Q VLANs allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

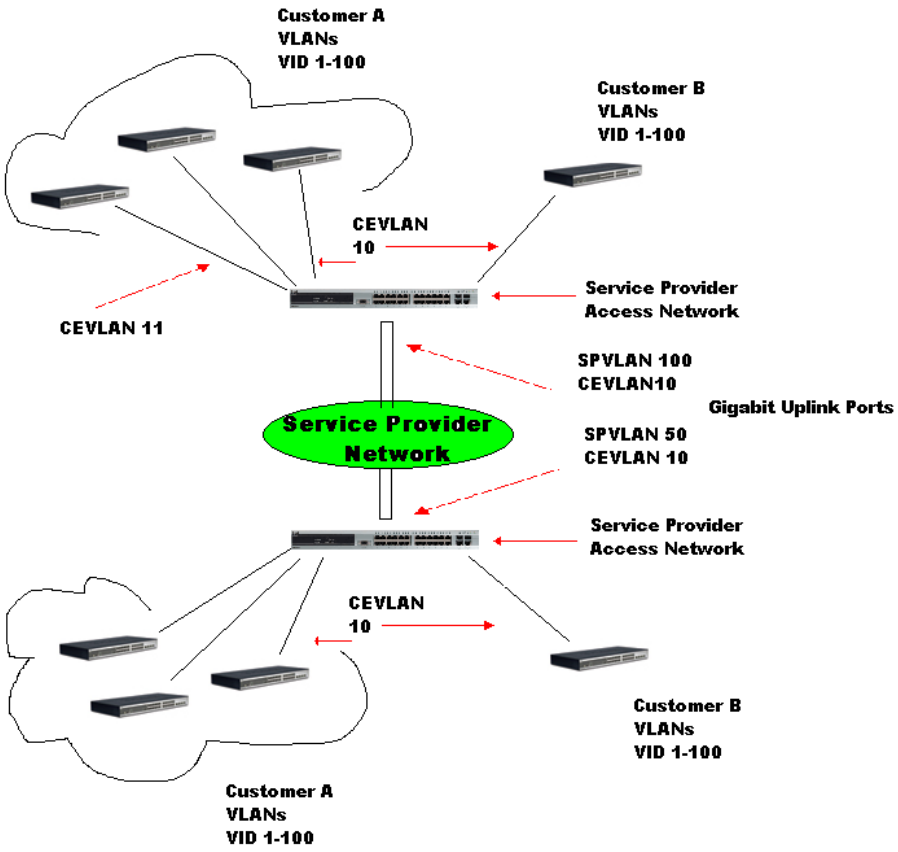
Double VLANs are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example Double VLAN tagged packet.

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload

Consider the example below:

Figure 74: QinQ example window



In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs. Both CEVLANs (Customer VLANs), 10 and 11, are tagged with the SPVID 100 on the Service Provider Access Network and therefore belong to one VLAN on the Service Provider's network, thus being a member of two VLANs. In this way, the Customer can retain its normal VLAN and the Service Provider can congregate multiple Customer VLANs within one SPVLAN, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for Double VLANs

Some rules and regulations apply with the implementation of the Double VLAN procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.

5 The switch cannot have both double and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.

6 Once Double VLANs are enabled, GVRP must be disabled.

7 All packets sent from the CPU to the Access ports must be untagged.

8 The following functions will not operate when the switch is in Double VLAN mode:

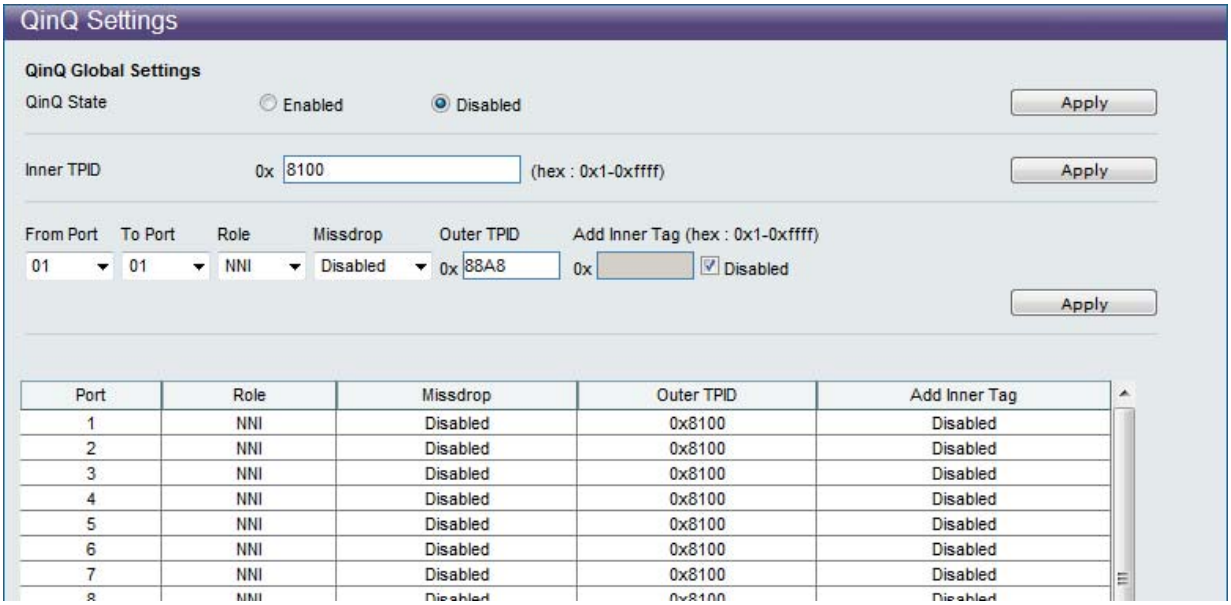
- Guest VLANs.
- Web-based Access Control.
- IP Multicast Routing.
- GVRP.
- All Regular 802.1Q VLAN functions.

QinQ Settings

On this page the user can configure the QinQ parameters.

To view the following window, click **L2 Features > QinQ > QinQ Settings**, as show below:

Figure 75: QinQ Settings Window



The fields that can be configured are described below:

Parameter	Description
QinQ State	Selecting this option enable the QinQ feature.
Inner TPID	Enter an Inner TPID in SP-VLAN tag here.
From Port – To Port	Here the user can select a range of ports to use in the configuration.
Role	Port role in QinQ mode, it can be UNI port or NNI port

Parameter	Description
Missdrop	This option enables or disables C-VLAN based SP-VLAN assignment miss drop. If Missdrop is enabled, the packet that does not match any assignment rule in the QinQ profile will be dropped. If disabled, then the packet will be forwarded and will be assigned to the PVID of the received port.
Outer TPID	Enter an Outer TPID in SP-VLAN tag here.
Add Inner Tag	Specifies that an Inner Tag will be added to the entry. By default the **Disabled** option is selected.

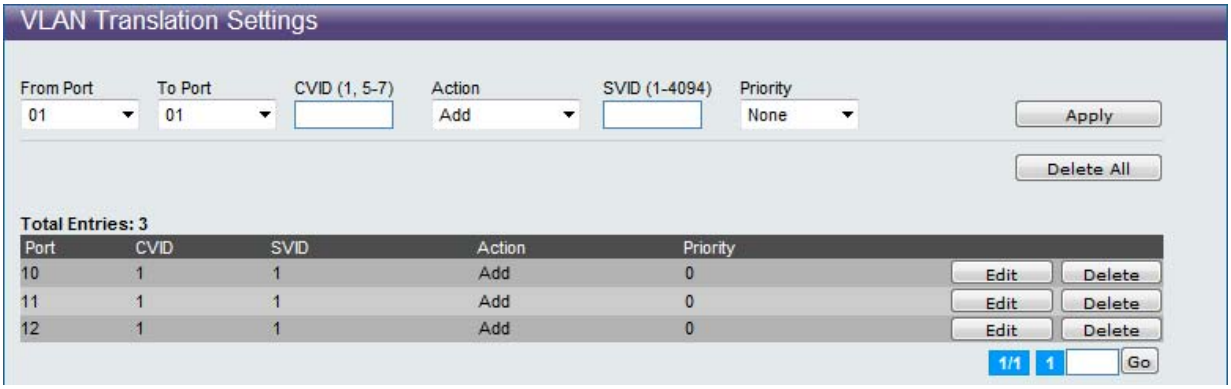
Click the **Apply** button to accept the changes made for each individual section.

VLAN Translation Settings

This page can be used to add translation relationship between C-VLAN and SP-VLAN. On ingress at UNI port, the C-VLAN tagged packets will be translated to SP-VLAN tagged packets by adding or replacing according the configured rule. On egress at this port, the SP-VLAN tag will be recovered to C-VLAN tag or be striped. The priority will be the priority in the SP-VLAN tag if the inner priority flag is disabled for the receipt port.

To view the following window, click **L2 Features > QinQ > VLAN Translation Settings**, as show below:

Figure 76: VLAN Translation Settings Window



The fields that can be configured are described below:

Parameter	Description
From Port – To Port	Here the user can select a range of ports to use in the configuration.
CVID	Here the user can enter the C-VLAN ID to match.
Action	The action indicates to add an S-tag before a C-tag or to replace the original C-tag by an S-tag.
SVID	Here the user can enter the SP-VLAN ID.
Priority	Here the user can select the priority of the s-tag.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove a specific entry.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP, and 802.1Q-2005 MSTP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP and 802.1Q-2005 MSTP have been recently introduced to Extreme managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP, and 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)
2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **MSTI Config Information** window when configuring MSTI ID settings).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in 802.1D-1998 and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 7-3 below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	*Discarding*	*Blocking*	No	No
Discarding	*Discarding*	*Listening*	No	No
Learning	*Learning*	*Learning*	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

1 On the switch level, the settings are globally implemented.

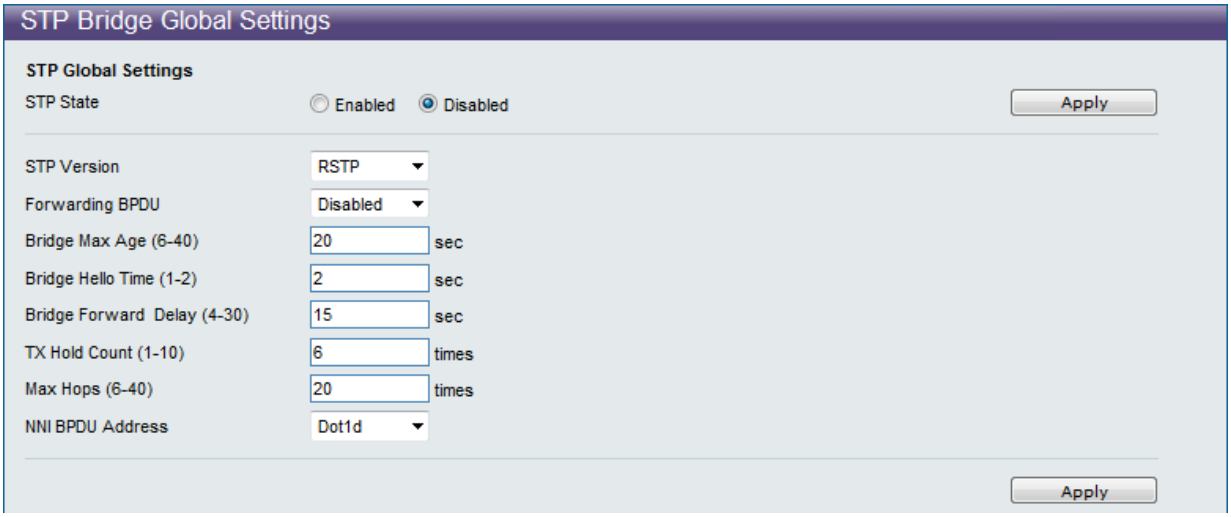
2 On the port level, the settings are implemented on a per-user-defined group of ports basis.

STP Bridge Global Settings

On this page the user can configure the STP bridge global parameters.

To view the following window, click **L2 Features > Spanning Tree > STP Bridge Global Settings**, as show below:

Figure 77: STP Bridge Global Settings window



The fields that can be configured are described below:

Parameter	Description
STP Status	Use the radio button to globally enable or disable STP.

Parameter	Description
STP Version	Use the pull-down menu to choose the desired version of STP: *STP* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *MSTP* - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.
Bridge Max Age (6 – 40)	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. The user may choose a time between *6* and *40* seconds. The default value is *20* seconds.
Bridge Hello Time (1 – 2)	The Hello Time can be set from *1* to *2* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis. The default is *2* seconds.
Bridge Forward Delay (4 – 30)	The Forward Delay can be from *4* to *30* seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state. The default is *15* seconds
Tx Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6*.
Max Hops (6-40)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from *6* to *40*. The default is *20*.
NNI BPDU Address	Used to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.

Click the **Apply** button to accept the changes made for each individual section.

NOTE

The Bridge Hello Time cannot be longer than the Bridge Max Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

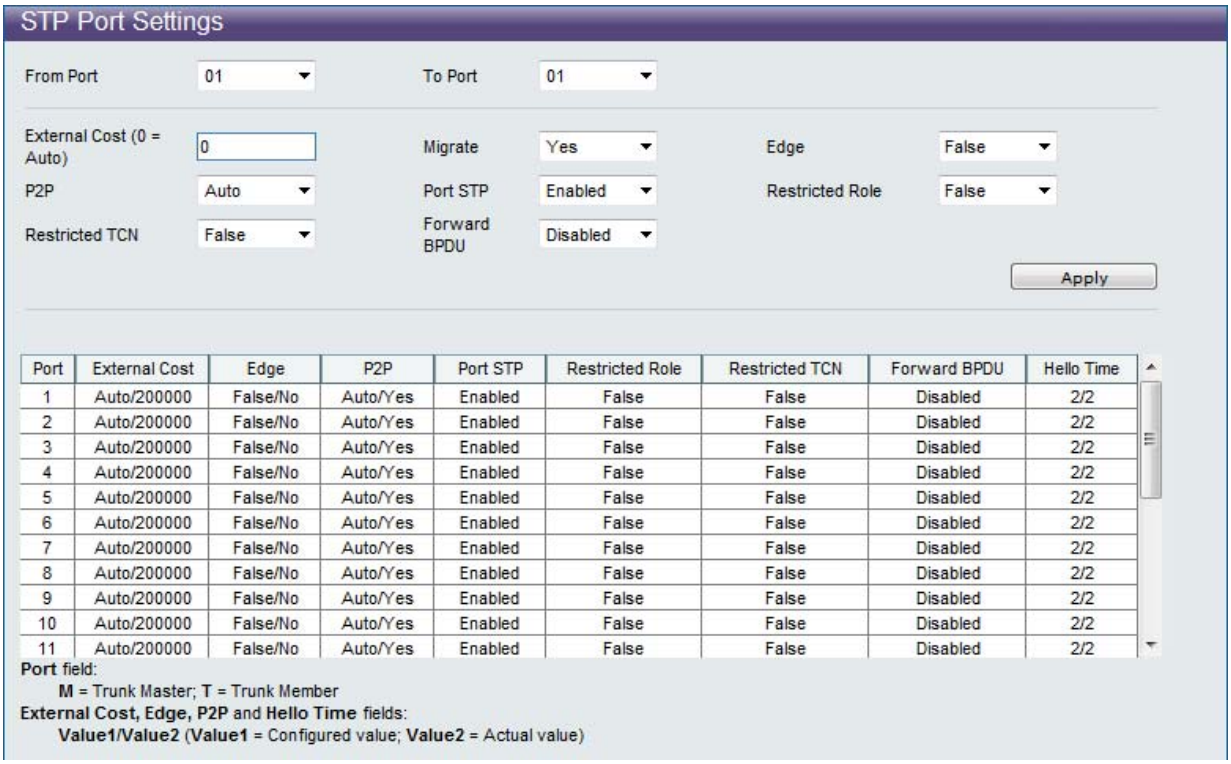
Bridge Max Age <= 2 x (Bridge Forward Delay - 1 second)
Bridge Max Age > 2 x (Bridge Hello Time + 1 second)

STP Port Settings

STP can be set up on a port per port basis.

To view the following window, click **L2 Features > Spanning Tree > STP Port Settings**, as show below

Figure 78: STP Port Settings window:



Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDU	Hello Time
1	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
2	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
3	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
4	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
5	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
6	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
7	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
8	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
9	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
10	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
11	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the starting and ending ports to be configured.
External Cost (0=Auto)	This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto). Setting *0* for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is *200000* and the default port cost for a Gigabit port is *20000*. Enter a value between *1* and *200000000* to determine the External Cost. The lower the number, the greater the probability the port will be chosen to forward packets.
P2P	Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports; however they are restricted in that a P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A P2P value of *False* indicates that the port cannot have P2P status. *Auto* allows the port to have P2P status whenever possible and operate as if the P2P status were *True*. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were *False*. The default setting for this parameter is *Auto*.

Parameter	Description
Restricted TCN	Topology Change Notification is a simple BPDU that a bridge sends out to its root port to signal a topology change. Restricted TCN can be toggled between *True* and *False*. If set to *True*, this stops the port from propagating received topology change notifications and topology changes to other ports. The default is *False*.
Migrate	When operating in RSTP mode, selecting *Yes* forces the port that has been selected to transmit RSTP BPDUs.
Port STP	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is *Enabled*.
Forward BPDU	Use the pull-down menu to enable or disable the flooding of BPDU packets when STP is disabled.
Edge	Choosing the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the *False* parameter indicates that the port does not have edge port status. Alternatively, the *Auto* option is available.
Restricted Role	Use the drop-down menu to toggle Restricted Role between *True* and *False*. If set to *True*, the port will never be selected to be the Root port. The default is *False*.

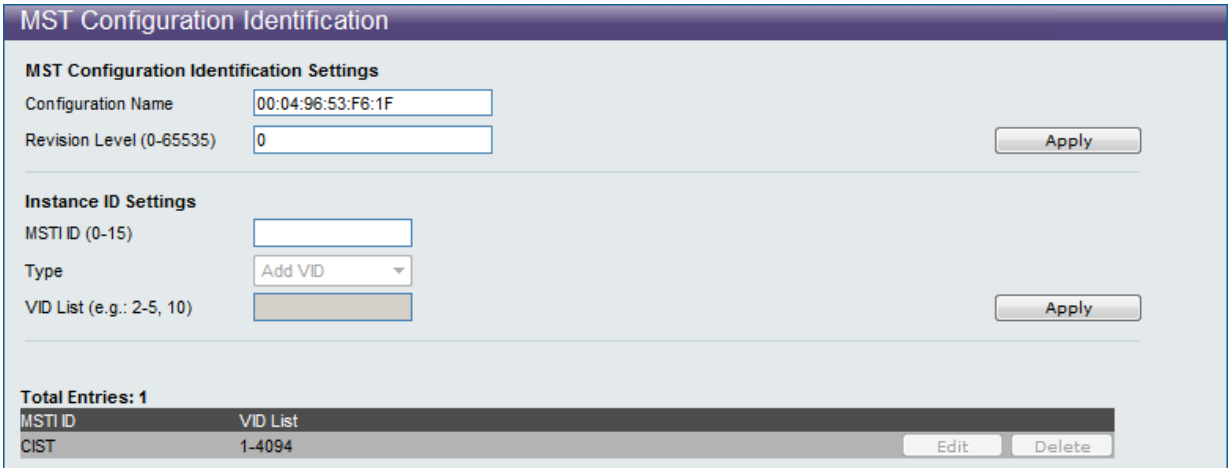
Click the **Apply** button to accept the changes made.

MST Configuration Identification

This window allows the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one CIST, or Common Internal Spanning Tree, of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

To view the following window, click **L2 Features > Spanning Tree > MST Configuration Identification**, as show below:

Figure 79: MST Configuration Identification window



The fields that can be configured are described below:

Parameter	Description
Configuration Name	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a Configuration Name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.
MSTI ID	Enter a number between *1* and *15* to set a new MSTI on the Switch.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices: *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number *1* to *4094*.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.

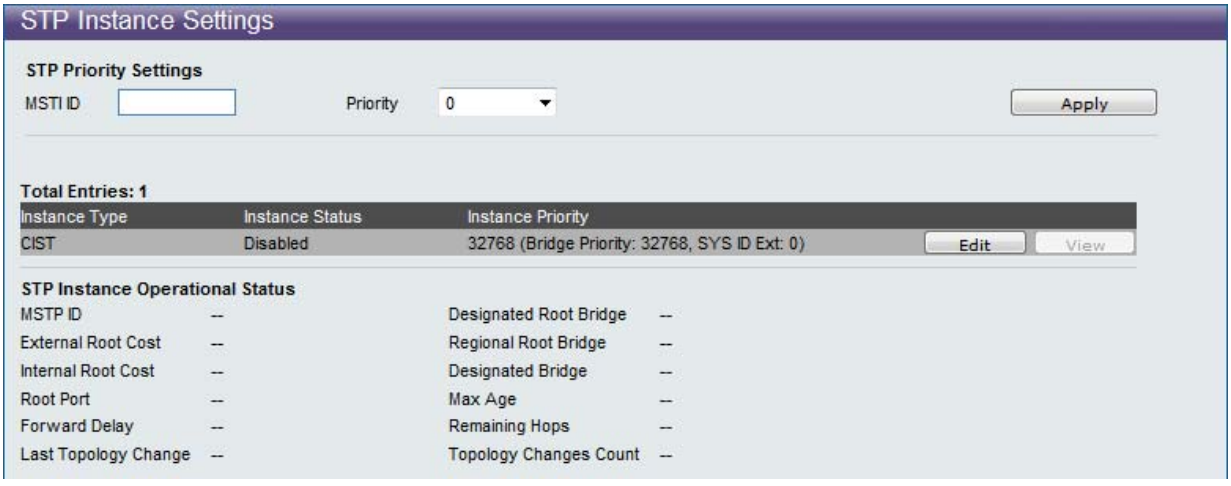
Click the **Delete** button to remove the specific entry.

STP Instance Settings

This window displays MSTIs currently set on the Switch and allows users to change the Priority of the MSTIs.

To view the following window, click **L2 Features > Spanning Tree > STP Instance Settings**, as show below:

Figure 80: STP Instance Settings window



The fields that can be configured are described below:

Parameter	Description
MSTI ID	Enter the MSTI ID in this field. An entry of *0* denotes the CIST (default MSTI).
Priority	Enter the priority in this field. The available range of values is from *0* to *61440*.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

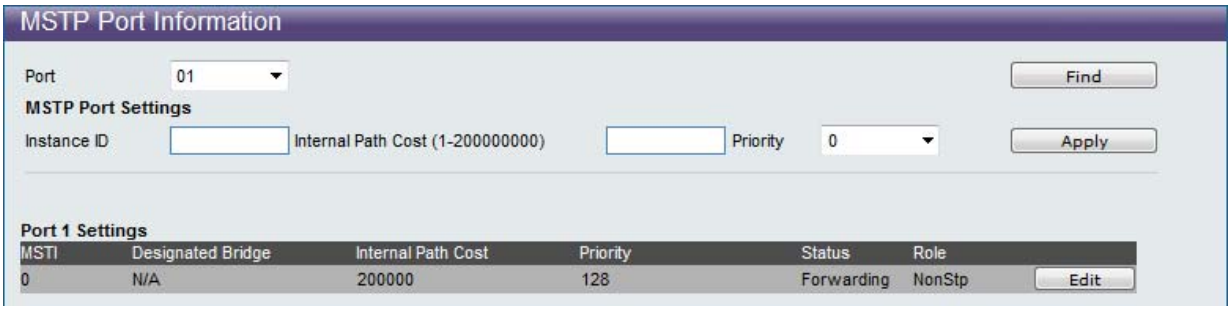
Click the **View** button to display the information of the specific entry.

MSTP Port Information

This window displays the current MSTI configuration information and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the following window, click **L2 Features > Spanning Tree > MSTP Port Information**, as show below:

Figure 81: MSTP Port Information window



To view the MSTI settings for a particular port, use the drop-down menu to select the Port number. To modify the settings for a particular MSTI instance, enter a value in the Instance ID field, an Internal Path Cost, and use the drop-down menu to select a Priority.

The fields that can be configured are described below:

Parameter	Description
Port	Select the port you want to configure.
Instance ID	The MSTI ID of the instance to be configured. Enter a value between *0* and *15*. An entry of *0* in this field denotes the CIST (default MSTI).
Internal Path Cost	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of *1* to *200000000* will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission. Selecting *0* (zero) for this parameter will set the quickest route automatically and optimally for an interface.

Parameter	Description
Priority	Enter a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Apply** button to accept the changes made.

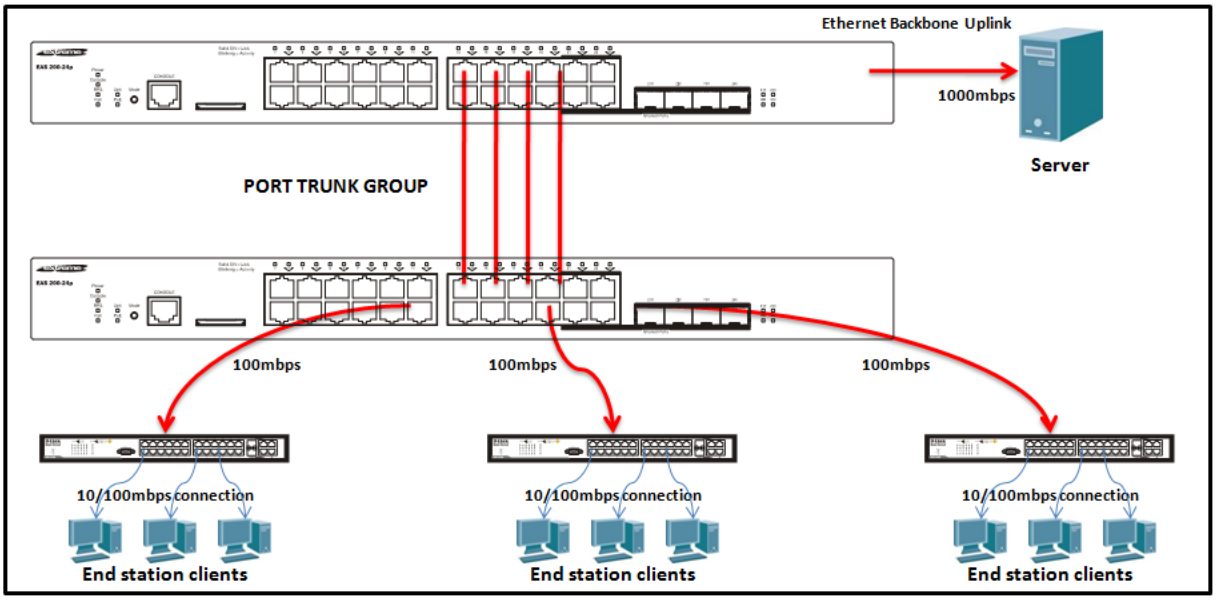
Click the **Edit** button to re-configure the specific entry.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to 12 port trunk groups with two to eight ports in each group. A potential bit rate of 8000 Mbps can be achieved.

Figure 82: Example of Port Trunk Group



The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The Switch allows the creation of up to 12 link aggregation groups, each group consisting of 2 to 8 links (ports). The (optional) Gigabit ports can only belong to a single link aggregation group.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.

NOTE

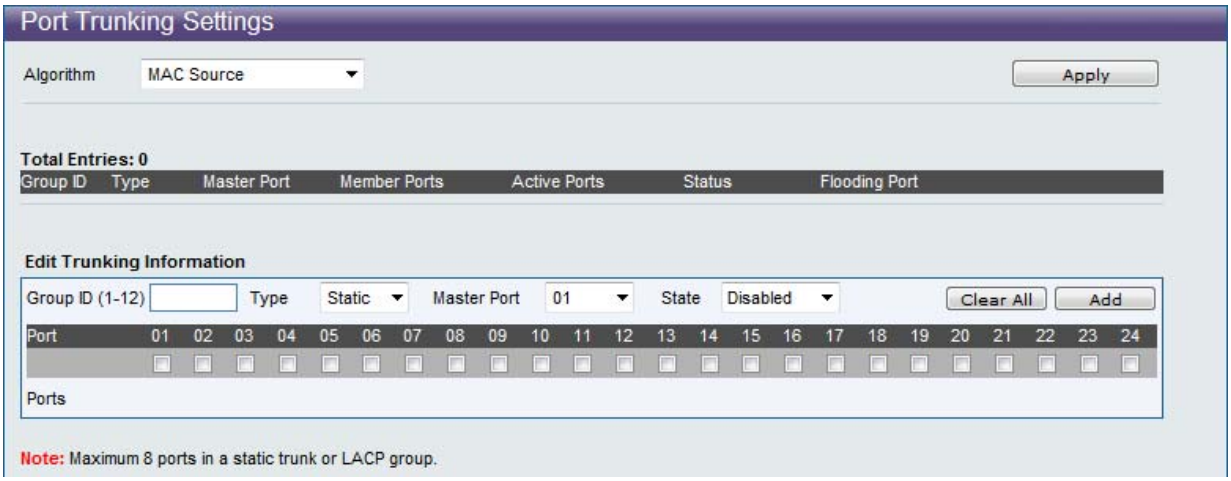
If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

Port Trunking Settings

On this page the user can configure the port trunk settings for the switch.

To view the following window, click **L2 Features > Link Aggregation > Port Trunking Settings**, as show below:

Figure 83: Port Trunking Settings window



The fields that can be configured are described below:

Parameter	Description
Algorithm	This is the traffic hash algorithm among the ports of the link aggregation group. Options to choose from are MAC Source Dest, IP Source Dest and Lay4 Source Dest.
Group ID (1-12)	Select an ID number for the group, between *1* and *12*.
Type	This pull-down menu allows users to select between *Static* and *LACP* (Link Aggregation Control Protocol). *LACP* allows for the automatic detection of links in a Port Trunking Group.
Master Port	Choose the Master Port for the trunk group using the drop-down menu.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Member Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Active Ports	Shows the ports that are currently forwarding packets.

Click the **Apply** button to accept the changes made.

Click the **Clear All** button to clear out all the information entered.

Click the **Add** button to add a new entry based on the information entered.

NOTE

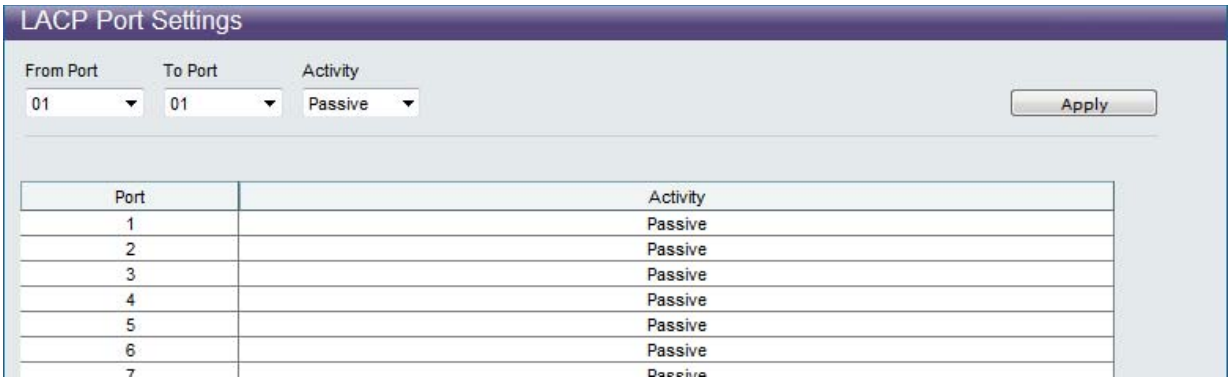
The maximum number of ports that can be configured in one Static Trunk or LACP Group are **8 ports**.

LACP Port Settings

In conjunction with the Trunking window, users can create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

To view the following window, click **L2 Features > Link Aggregation > LACP Port Settings**, as show below:

Figure 84: LACP Port Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	A consecutive group of ports may be configured starting with the selected port.
Activity	*Active* - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. *Passive* - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above).

Click the **Apply** button to accept the changes made.

FDB

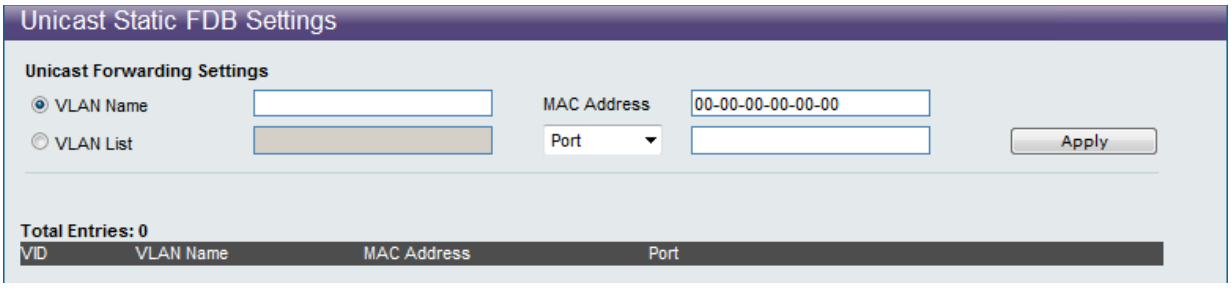
Static FDB Settings

Unicast Static FDB Settings

Users can set up static unicast forwarding on the Switch.

To view the following window, click **L2 Features > FDB > Static FDB Settings > Unicast Static FDB Settings**, as show below:

Figure 85: Unicast Static FDB Settings window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the radio button and enter the VLAN name of the VLAN on which the associated unicast MAC address resides.
VLAN List	Click the radio button and enter a list of VLAN on which the associated unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port/Drop	Allows the selection of the port number on which the MAC address entered above resides This option could also drop the MAC address from the unicast static FDB. When selecting *Port*, enter the port number in the field.

Click the **Apply** button to accept the changes made.

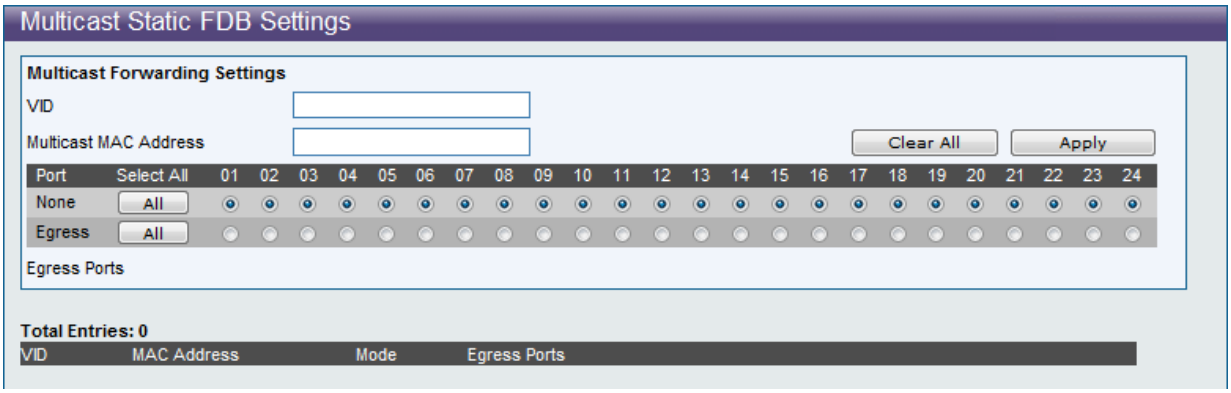
Click the **Delete** button to remove the specific entry.

Multicast Static FDB Settings

Users can set up static multicast forwarding on the Switch.

To view the following window, click **L2 Features > FDB > Static FDB Settings > Multicast Static FDB Settings**, as show below:

Figure 86: Multicast Static FDB Settings window



The fields that can be configured are described below:

Parameter	Description
VID	The VLAN ID of the VLAN the corresponding MAC address belongs to.
Multicast MAC Address	The static destination MAC address of the multicast packets. This must be a multicast MAC address.
Port	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are: *None* - No restrictions on the port dynamically joining the multicast group. When *None* is chosen, the port will not be a member of the Static Multicast Group. Click the **All** button to select all the ports. *Egress* - The port is a static member of the multicast group. Click the **All** button to select all the ports.

Click the **Clear All** button to clear out all the information entered.

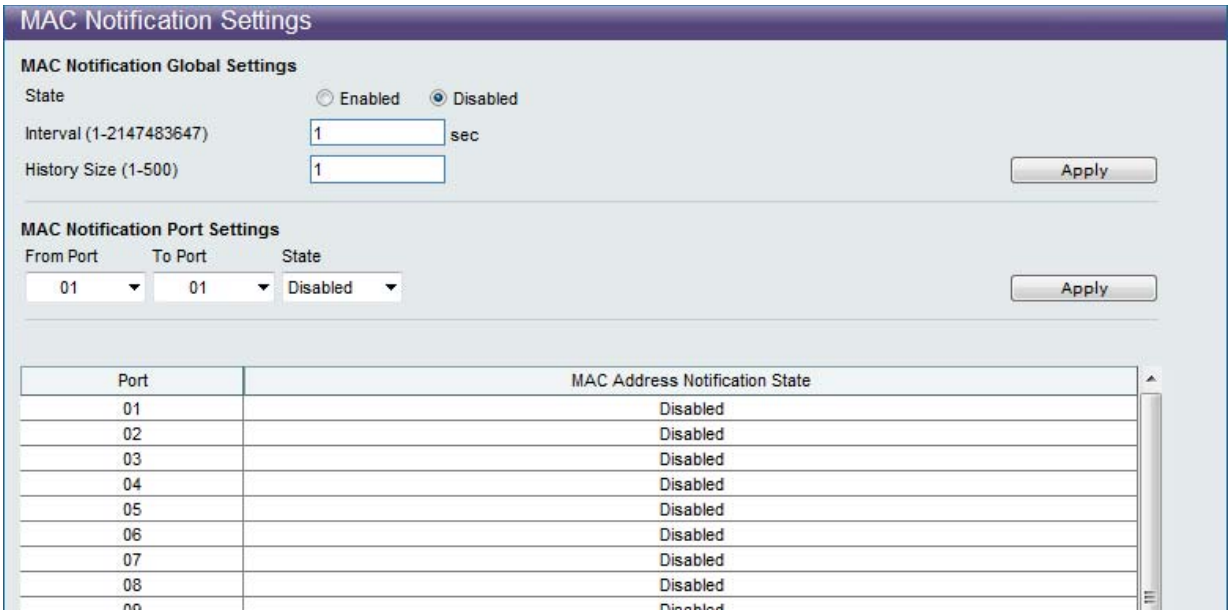
Click the **Apply** button to accept the changes made.

MAC Notification Settings

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database. This window allows you to globally set MAC notification on the Switch. Users can set MAC notification for individual ports on the Switch.

To view the following window, click **L2 Features > FDB > MAC Notification Settings**, as show below:

Figure 87: MAC Notification Settings window



The fields that can be configured are described below:

Parameter	Description
State	Enable or disable MAC notification globally on the Switch
Interval	The time in seconds between notifications. Value range to use is *1* to *2147483647*.
History Size	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.
From Port / To Port	Select the starting and ending ports for MAC notification.
State	Enable MAC Notification for the ports selected using the pull-down menu.

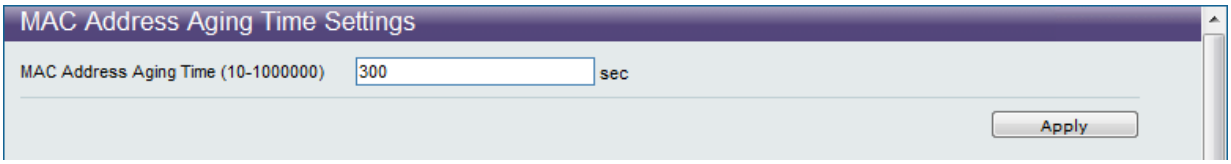
Click the **Apply** button to accept the changes made for each individual section.

MAC Address Aging Time Settings

Users can configure the MAC Address aging time on the Switch.

To view the following window, click **L2 Features > FDB > MAC Address Aging Time Settings**, as show below:

Figure 88: MAC Address Aging Time Settings window



The fields that can be configured are described below:

Parameter	Description
MAC Address Aging Time (10-1000000)	This field specify the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this option, type in a different value representing the MAC address' age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1000000* seconds. The default setting is *300* seconds.

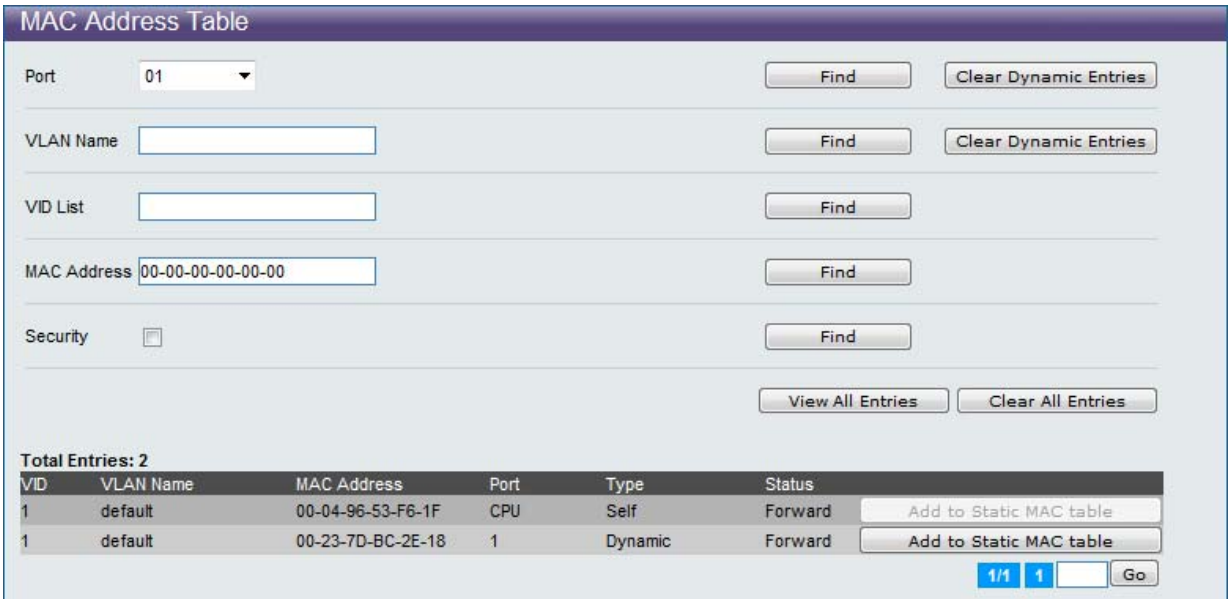
Click the **Apply** button to accept the changes made.

MAC Address Table

This allows the Switch's MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address, VLAN and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

To view the following window, click **L2 Features > FDB > MAC Address Table**, as show below:

Figure 89: MAC Address Table window



The fields that can be configured are described below:

Parameter	Description
Port	The port to which the MAC address below corresponds.
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Dynamic Entries** button to delete all dynamic entries of the address table.

Click the **View All Entries** button to display all the existing entries.

Click the **Clear All Entries** button to remove all the entries listed in the table.

Click the **Add to Static MAC table** button to add the specific entry to the Static MAC table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP & FDB Table

On this page the user can find the ARP and FDB table parameters.

To view the following window, click **L2 Features > FDB > ARP & FDB Table**, as show below:

Figure 90: ARP & FDB Table window

The fields that can be configured are described below:

Parameter	Description
Port	Select the port number to use for this configuration.
MAC Address	Enter the MAC address to use for this configuration.
IP Address	Enter the IP address the use for this configuration.

Click the **Find by Port** button to locate a specific entry based on the port number selected.

Click the **Find by MAC** button to locate a specific entry based on the MAC address entered.

Click the **Find by IP Address** button to locate a specific entry based on the IP address entered.

Click the **View All Entries** button to display all the existing entries.

Click the **Add to IP MAC Port Binding Table** to add the specific entry to the window.

L2 Multicast Control

IGMP Snooping

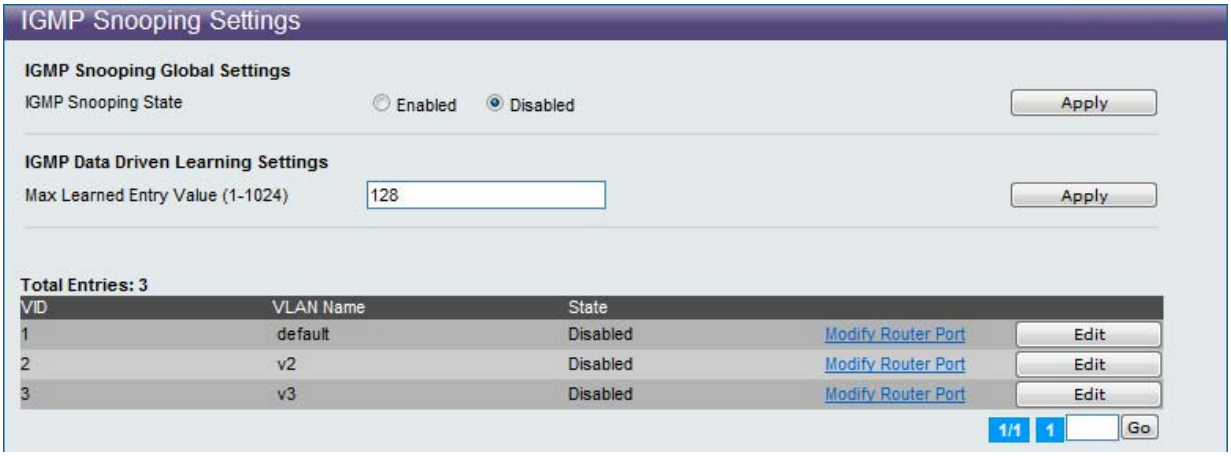
Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch under IGMP Global Settings at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings**, as show below:

Figure 91: IGMP Snooping Settings window



The fields that can be configured are described below:

Parameter	Description
IGMP Snooping State	Here the user can enable or disable the IGMP Snooping state.
Max Learning Entry Value	Here the user can enter the maximum learning entry value.

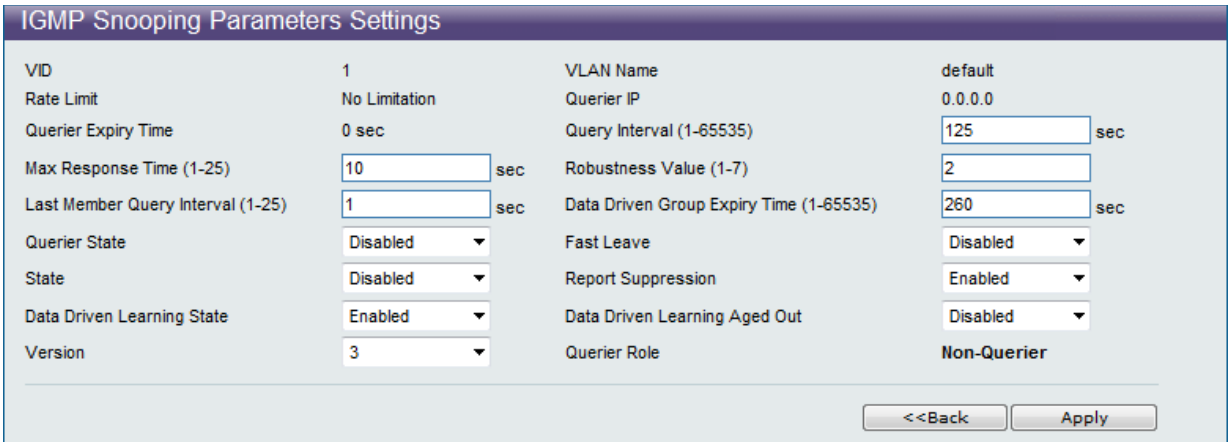
Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to configure the IGMP Snooping Parameters Settings.

Click the **Modify Router Port** link to configure the IGMP Snooping Router Port Settings.

After clicking the **Edit** button, the following page will appear:

Figure 92: IGMP Snooping Parameters Settings window



The fields that can be configured are described below:

Parameter	Description
VID	Specify the name of the VLAN ID.
VLAN Name	Specify the name of the VLAN for which IGMP snooping querier is to be configured.
Rate Limit	Here is displayed the rate of IGMP control packets that the switch can process on a specific port/VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.
Querier IP	Displays the querier IP address
Querier Expiry Time	Displays the querier expiry time.
Query Interval	Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds..
Max Response Time	Specify the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.
Robustness Value	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness value is used in calculating the following IGMP message intervals: By default, the robustness variable is set to 2.
Last Member Query Interval	Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.
Data Drive Group Expiry Time	Specify the data driven group lifetime in seconds.
Querier State	Specify to enable or disable the querier state.
Fast Leave	Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.

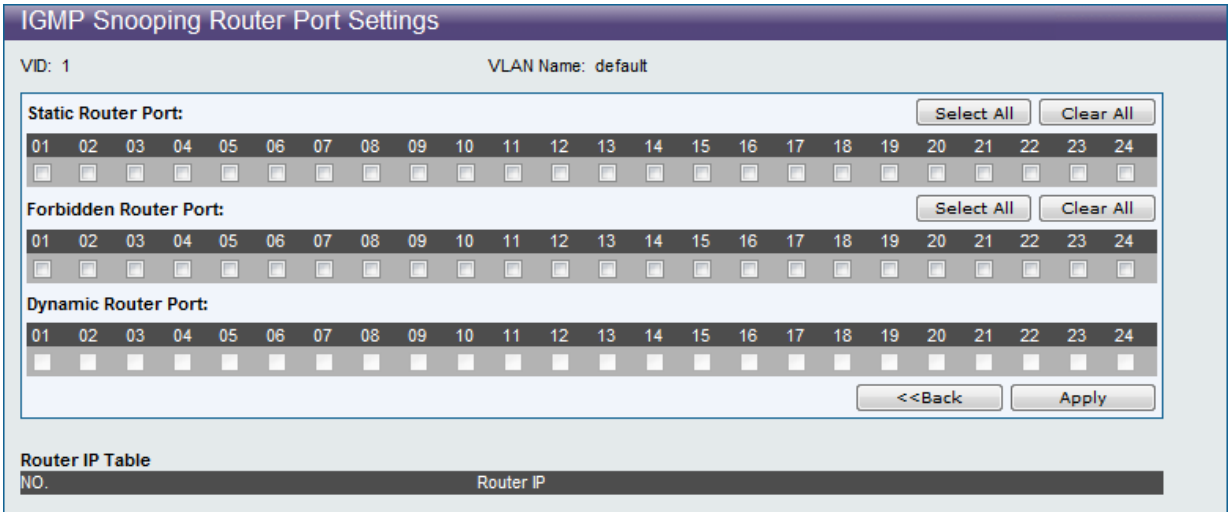
Parameter	Description
State	If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). It the state is disabled, then the switch can not play the role as a querier. **NOTE:** that if the Layer 3 router connected to the switch provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.
Report Suppression	When enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port.
Data Driven Learning State	Specify to enable or disable the data driven learning state.
Data Drive Learning Aged Out	Specify to enable or disable the data drive learning aged out option.
Version	Specify the version of IGMP packet that will be sent by this port. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.
Querier Role	Displays the querier role.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Modify Router Port** link, the following page will appear:

Figure 93: IGMP Snooping Router Port Settings window


IGMP Snooping Router Port Settings
VID: 1
VLAN Name: default
Static Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Forbidden Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply
Router IP Table
NO.
Router IP

The fields that can be configured are described below:

Parameter	Description
Static Router Port	This section is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router regardless of the protocol.

Parameter	Description
Forbidden Router Port	This section is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Dynamic Router Port	Displays router ports that have been dynamically configured.
Ports	Select the appropriate ports individually to include them in the Router Port configuration.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

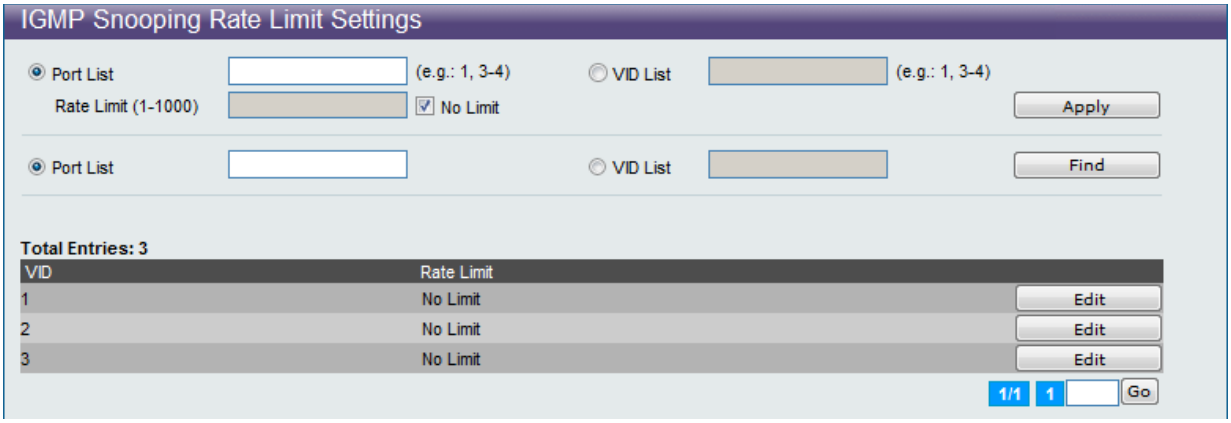
Click the **<<Back** button to discard the changes made and return to the previous page.

IGMP Snooping Rate Limit Settings

On this page the user can configure the IGMP snooping rate limit parameters.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Rate Limit Settings**, as show below:

Figure 94: IGMP Snooping Rate Limit Settings window



The fields that can be configured are described below:

Parameter	Description
Port List	Here the user can enter the port list used for this configuration.
VID List	Here the user can enter the VID list used for this configuration.
Rate Limit	Here the user can enter the IGMP snooping rate limit used. By selecting the **No Limit** option, the rate limit for the entered port(s) will be ignored.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

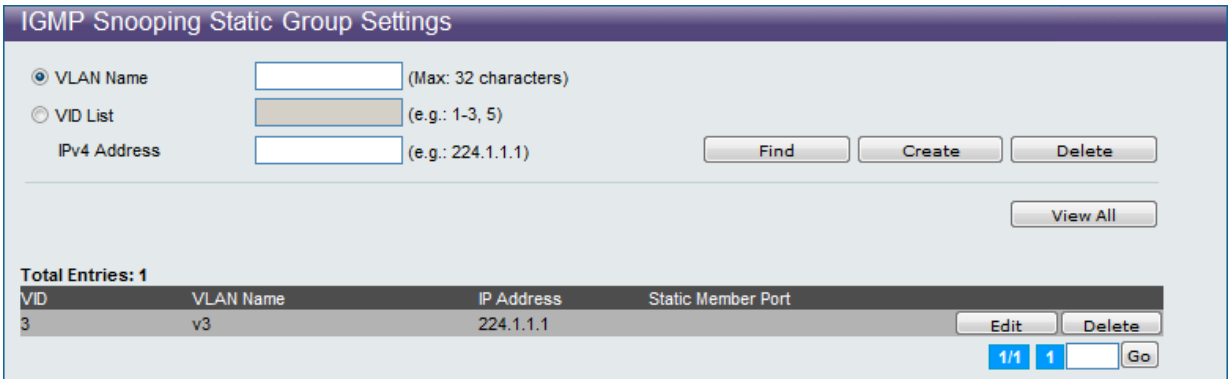
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IGMP Snooping Static Group Settings

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Static Group Settings**, as show below:

Figure 95: IGMP Snooping Static Group Settings window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	The *VLAN Name* of the multicast group.
VID List	The *VID List* or of the multicast group.
IPv4 Address	Enter the IPv4 address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Create** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

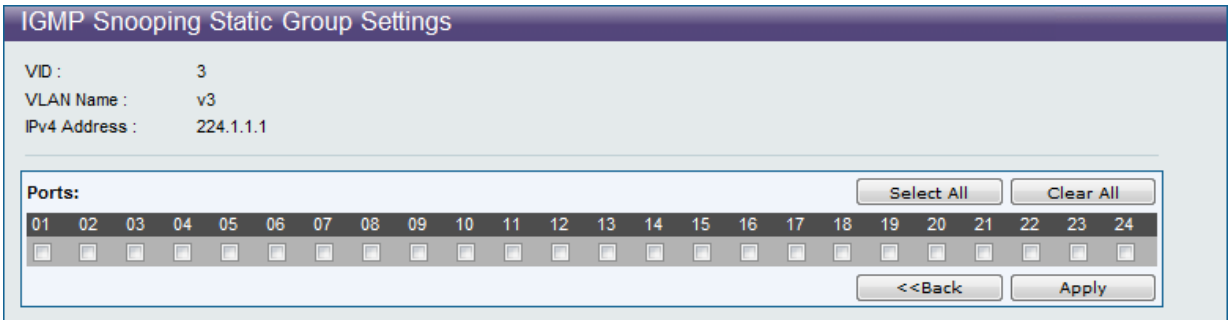
Click the **View All** button to display all the existing entries.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear:

Figure 96: IGMP Snooping Static Group Settings window


IGMP Snooping Static Group Settings
VID : 3
VLAN Name : v3
IPv4 Address : 224.1.1.1
Ports:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

IGMP Router Port

Users can display which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Router Port**, as show below:

Figure 97: IGMP Router Port window

IGMP Router Port
VID
Find
VID 1
VLAN Name default
Total Entries: 3
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1/3 1 2 3 > >>
Go
Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port

Enter a VID (VLAN ID) in the field at the top of the window.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

NOTE

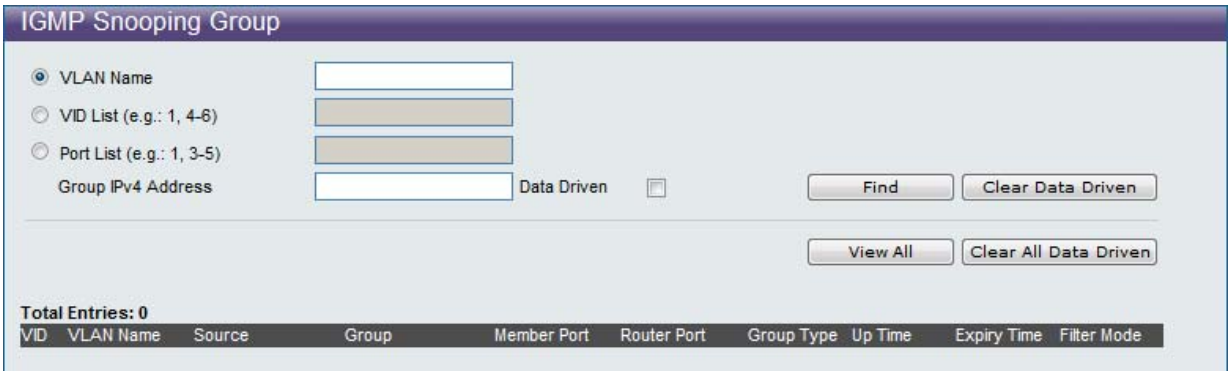
The abbreviations used on this page are **Static Router Port (S)**, **Dynamic Router Port (D)** and **Forbidden Router Port (F)**.

IGMP Snooping Group

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group**, as show below:

Figure 98: IGMP Snooping Group window



The user may search the IGMP Snooping Group Table by either *VLAN Name* or *VID List* by entering it in the top left hand corner and clicking **Find**.

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.
Port List	Specify the port number(s) used to find a multicast group.
Group IPv4 Address	Enter the IPv4 address.
Data Driven	If Data Drive is selected, only data driven groups will be displayed.

Click the **Clear Data Driven** button to delete the specific IGMP snooping group which is learned by the Data Driven feature of the specified VLAN.

Click the **View All** button to display all the existing entries.

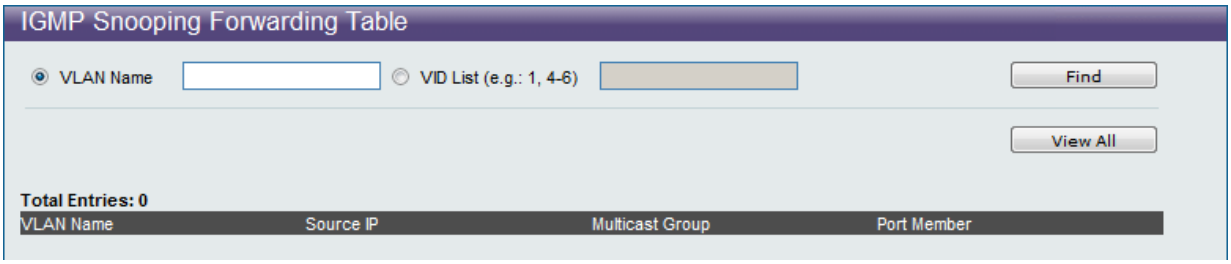
Click the **Clear All Data Driven** button to delete all IGMP snooping groups which is learned by the Data Driven feature of specified VLANs.

IGMP Snooping Forwarding Table

This page displays the switch's current IGMP snooping forwarding table. It provides an easy way for user to check the list of ports that the multicast group comes from and specific sources that it will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Forwarding Table**, as show below:

Figure 99: IGMP Snooping Forwarding Table window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.

Click the **Find** button to locate a specific entry based on the information entered.

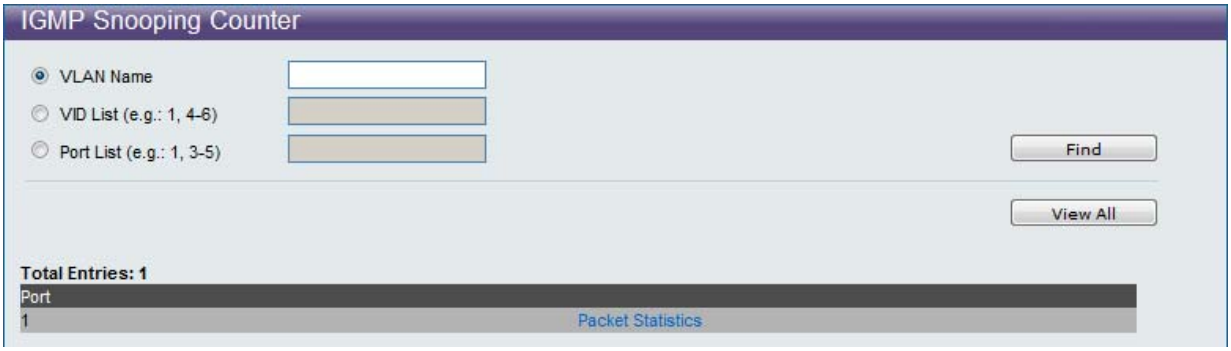
Click the **View All** button to display all the existing entries.

IGMP Snooping Counter

Users can view the switch's IGMP Snooping counter table.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Counter**, as show below:

Figure 100: IGMP Snooping Counter window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.
Port List	The *Port List* of the multicast group.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Packet Statistics** link to view the IGMP Snooping Counter Table.

After clicking the **Packet Statistics** link, the following page will appear:

Figure 101: Browse IGMP Snooping Counter window

Click the **Clear Counter** button to clear all the information displayed in the fields.

Click the **Refresh** button to refresh the display table so that new information will appear.

Click the **<<Back** button to return to the previous page.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

1 **Multicast Listener Query** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.

2 **Multicast Listener Report, Version 1** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

3 **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

4 **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

Data Driven Learning

The Switch allows you to implement data driven learning for MLD snooping groups. If data-driven learning, also known as dynamic IP multicast learning, is enabled for a VLAN, when the Switch receives IP multicast traffic on the VLAN, an MLD snooping group is created. Learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to age out or to age out by a timer.

When the data driven learning State is enabled, the multicast filtering mode for all ports is ignored. This means multicast packets will be flooded.

NOTE

If a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. In other words, the aging out mechanism will follow the conditions of an ordinary MLD snooping entry.

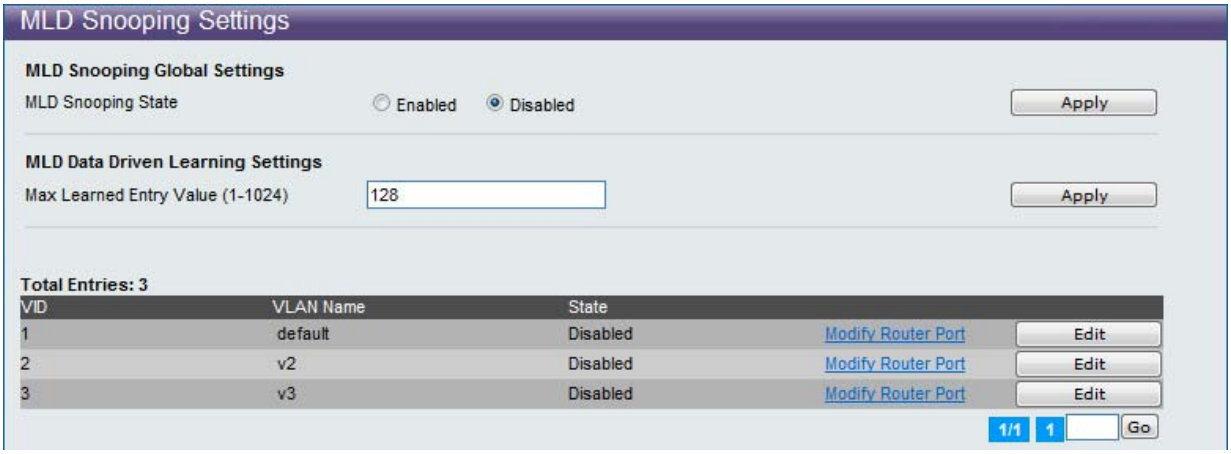
Data driven learning is useful on a network which has video cameras connected to a Layer 2 switch that is recording and sending IP multicast data. The switch needs to forward IP data to a data centre without dropping or flooding any packets. Since video cameras do not have the capability to run MLD protocols, the IP multicast data will be dropped with the original MLD snooping function.

MLD Snooping Settings

Users can configure the settings for MLD snooping.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings**, as show below:

Figure 102: MLD Snooping Settings window



The fields that can be configured are described below:

Parameter	Description
MLD Snooping State	Click the radio buttons to enable or disable the MLD snooping state.
Max Learning Entry Value	Enter the maximum learning entry value.

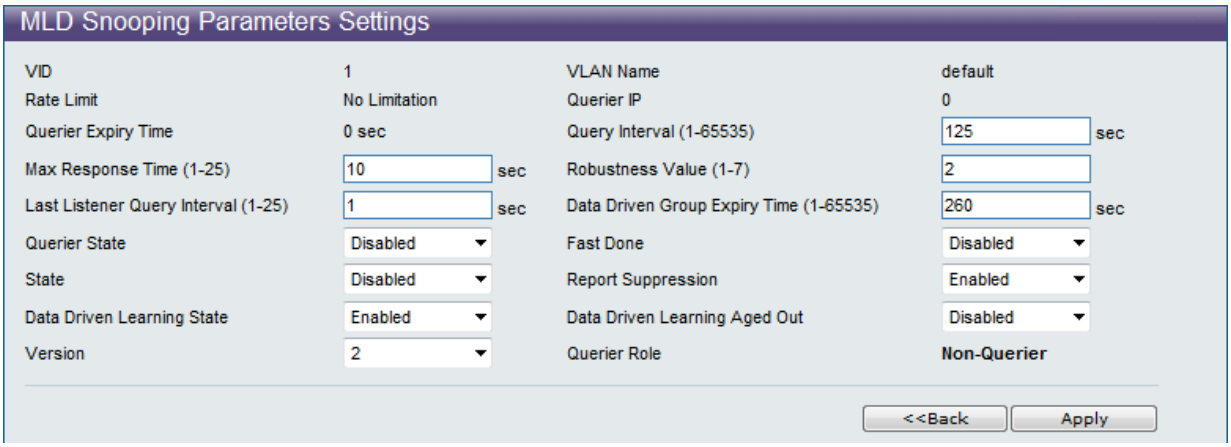
Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to configure the MLD Snooping Parameters Settings for a specific entry.

Click the **Modify Router Port** link to configure the MLD Snooping Router Port Settings for a specific entry.

After clicking the **Edit** button, the following page will appear:

Figure 103: MLD Snooping Parameters Settings window



The fields that can be configured are described below:

Parameter	Description
Query Interval	Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
Max Response Time	The maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.
Robustness Value	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: *Group listener interval* - Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. *Other Querier present interval* - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the Querier. *Last listener query count* - Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.
Last Listener Query Interval	The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.
Data Driven Group Expiry Time	Here the user can enter the data driven group expiry time value.
Querier State	This allows the switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.
Fast Done	Here the user can enable or disable the fast done feature.
State	Used to enable or disable MLD snooping for the specified VLAN. This field is *Disabled* by default.
Report Suppression	Here the user can enable or disable the report suppression features.
Data Driven Learning State	Enable or disable data driven learning of MLD snooping groups.
Data Driven Learning Aged Out	Enable or disable the age out function for data driven entries.

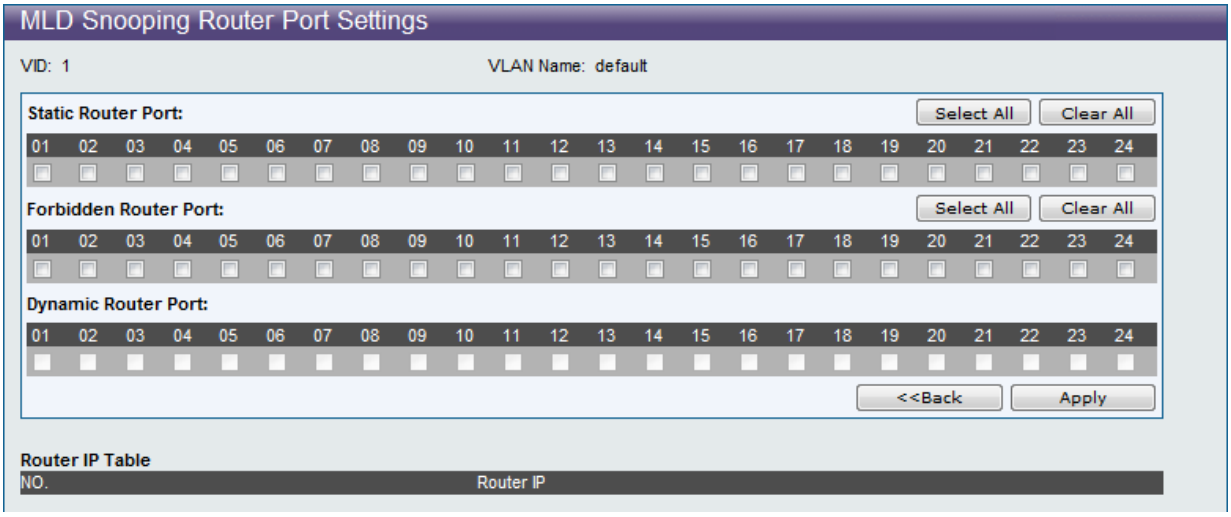
Parameter	Description
Version	Specify the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Modify Router Port** link, the following page will appear:

Figure 104: MLD Snooping Router Port Settings window


MLD Snooping Router Port Settings
VID: 1
VLAN Name: default
Static Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Forbidden Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply
Router IP Table
NO.
Router IP

The fields that can be configured are described below:

Parameter	Description
Static Router Port	This section is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router regardless of the protocol.
Forbidden Router Port	This section is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Dynamic Router Port	Displays router ports that have been dynamically configured.
Ports	Select the appropriate ports individually to include them in the Router Port configuration.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

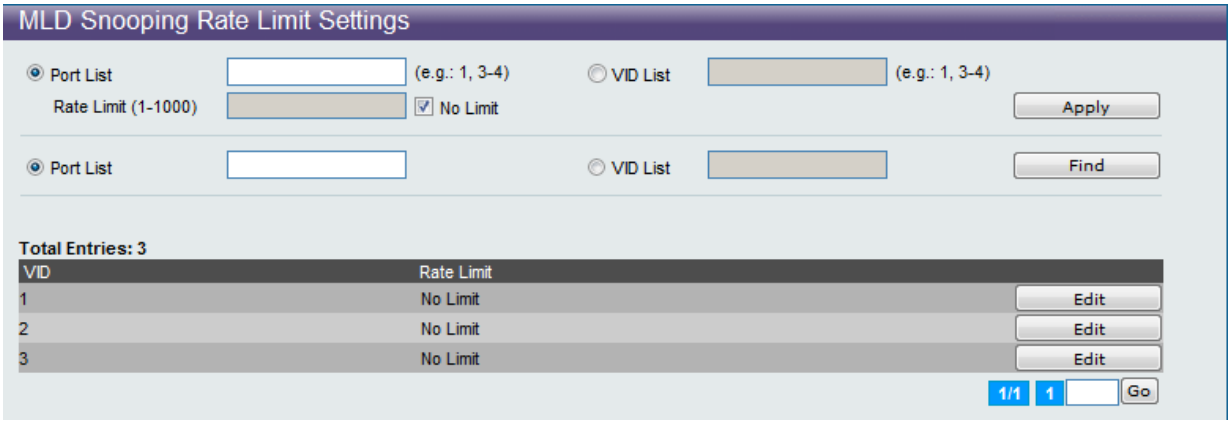
Click the **<<Back** button to discard the changes made and return to the previous page.

MLD Snooping Rate Limit Settings

Users can configure the rate limit of the MLD control packet that the switch can process on a specific port or VLAN in this page.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Rate Limit Settings**, as show below:

Figure 105: MLD Snooping Rate Limit Settings window



The fields that can be configured are described below:

Parameter	Description
Port List	Enter the Port List here.
VID List	Enter the VID List value here.
Rate Limit	Configure the rate limit of MLD control packet that the switch can process on a specific port/VLAN. The rate is specified in packet per second. The packet that exceeds the limited rate will be dropped. Selecting the **No Limit** option lifts the rate limit requirement.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Find** button to locate a specific entry based on the information entered.

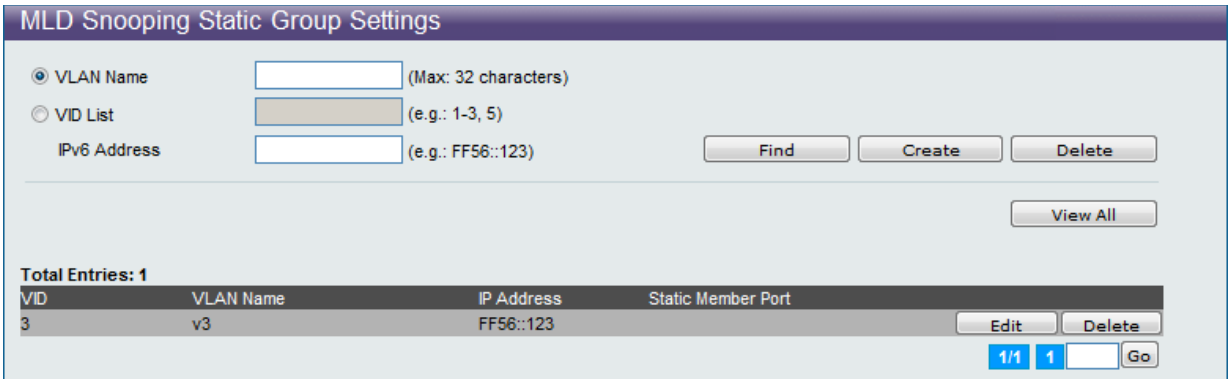
Click the **Edit** button to re-configure the specific entry.

MLD Snooping Static Group Settings

This page used to configure the MLD snooping multicast group static members.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Static Group Settings**, as show below:

Figure 106: MLD Snooping Static Group Settings window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	The name of the VLAN on which the static group resides.
VID List	The ID of the VLAN on which the static group resides.
IPv6 Address	Specify the multicast group IPv6 address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Create** button to add a static group.

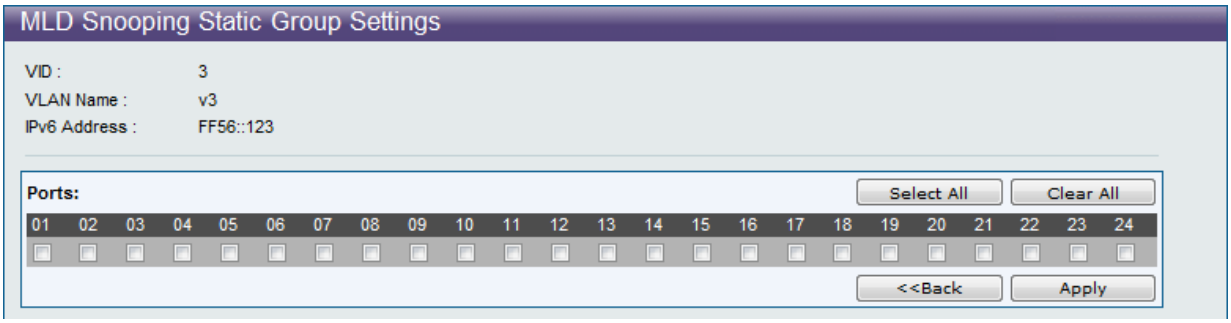
Click the **Delete** button to delete a static group.

Click the **View All** button to display all the existing entries.

Click the **Edit** button to re-configure the specific entry.

After clicking the **Edit** button, the following page will appear:

Figure 107: MLD Snooping Static Group Settings – Edit window



Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

MLD Router Port

Users can display which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Router Port**, as show below:

Figure 108: MLD Router Port window

MLD Router Port
VID
Find
VID 1
VLAN Name default
Total Entries: 3
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1/3 1 2 3 > >>
Go
Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port

Enter a **VID** (VLAN ID) in the field at the top of the window.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

NOTE

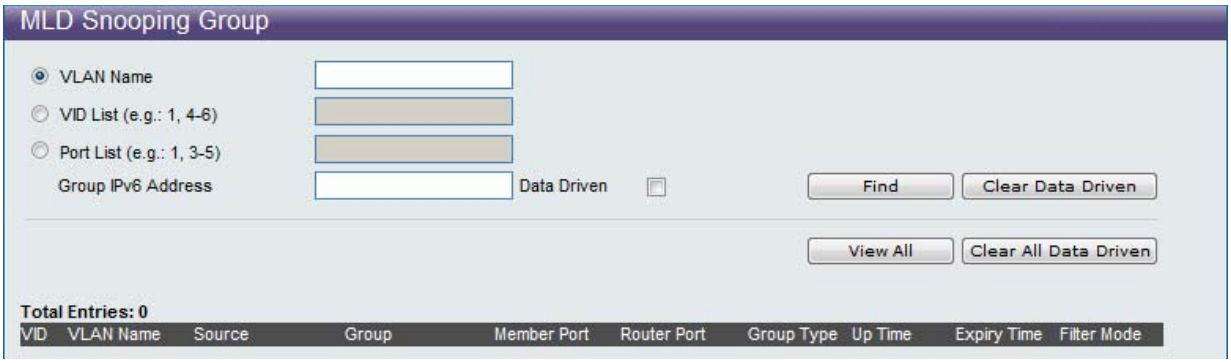
The abbreviations used on this page are **Static Router Port (S)**, **Dynamic Router Port (D)** and **Forbidden Router Port (F)**.

MLD Snooping Group

Users can view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Group**, as show below:

Figure 109: MLD Snooping Group window


MLD Snooping Group
VLAN Name
VID List (e.g.: 1, 4-6)
Port List (e.g.: 1, 3-5)
Group IPv6 Address
Data Driven
Find
Clear Data Driven
View All
Clear All Data Driven
Total Entries: 0
VID VLAN Name Source Group Member Port Router Port Group Type Up Time Expiry Time Filter Mode

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the radio button and enter the VLAN name of the multicast group.
VID List	Click the radio button and enter a VLAN list of the multicast group.
Port List	Specify the port number(s) used to find a multicast group.
Group IPv6 Address	Enter the group IPv6 address used here. Select the **Data Driven** option to enable the data driven feature for this MLD snooping group.
Data Driven	If Data Drive is selected, only data driven groups will be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Data Driven** button to delete the specific MLD snooping group which is learned by the Data Driven feature of the specified VLAN.

Click the **View All** button to display all the existing entries.

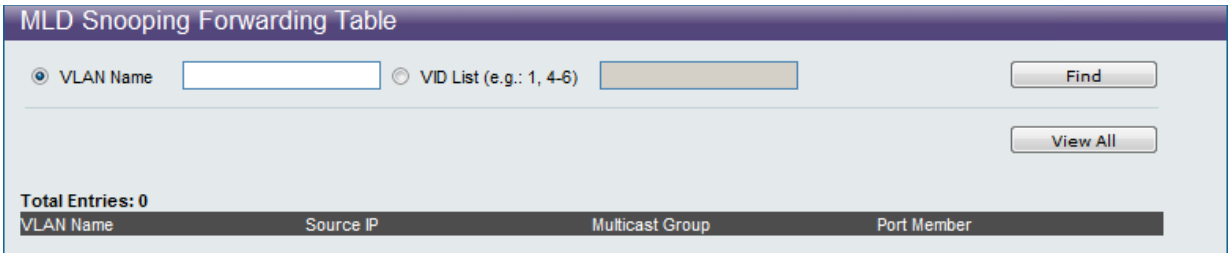
Click the **Clear All Data Driven** button to delete all MLD snooping groups which is learned by the Data Driven feature of specified VLANs.

MLD Snooping Forwarding Table

This page displays the switch's current MLD snooping forwarding table. It provides an easy way for user to check the list of ports that the multicast group comes from and specific sources that it will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The MLD snooping further restricts the forwarding ports.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Forwarding Table**, as show below:

Figure 110: MLD Snooping Forwarding Table window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	The name of the VLAN for which you want to view MLD snooping forwarding table information.
VID List	The ID of the VLAN for which you want to view MLD snooping forwarding table information.

Click the **Find** button to locate a specific entry based on the information entered.

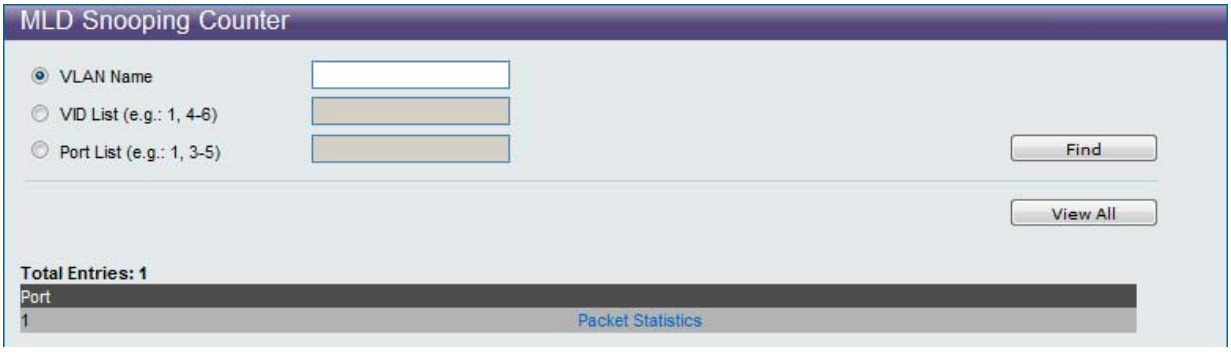
Click the **View All** button to display all the existing entries.

MLD Snooping Counter

This page displays the statistics counter for MLD protocol packets that are received by the switch since MLD Snooping is enabled.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Counter**, as show below:

Figure 111: MLD Snooping Counter window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	Specify a VLAN name to be displayed.

Parameter	Description
VID List	Specify a list of VLANs to be displayed.
Port List	Specify a list of ports to be displayed.

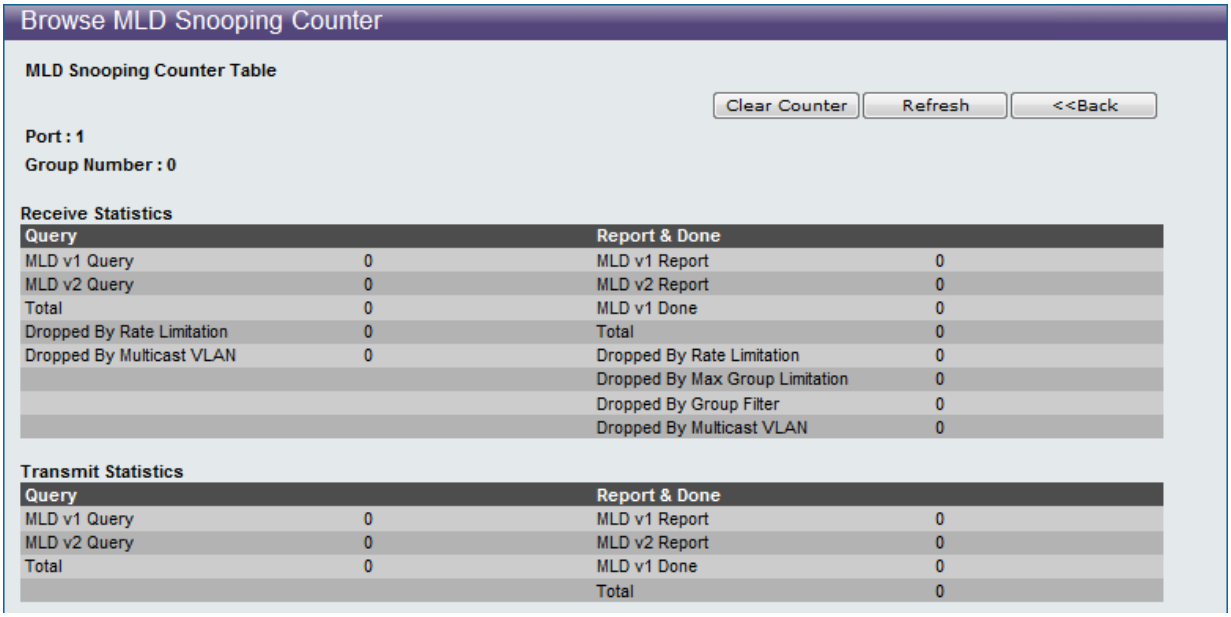
Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Packet Statistics** link to view the MLD Snooping Counter Settings for the specific entry.

After clicking the **Packet Statistics** link, the following page will appear:

Figure 112: Browse MLD Snooping Counter window



Click the **Clear Counter** button to clear all the information displayed in the fields.

Click the **Refresh** button to refresh the display table so that new information will appear.

Click the **<<Back** button to return to the previous page.

Multicast Filtering

IPv4 Multicast Filtering

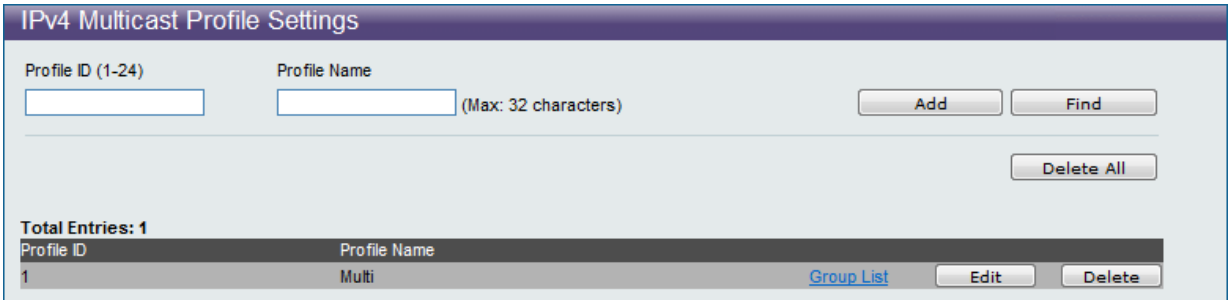
IPv4 Multicast Profile Settings

Users can add a profile to which multicast address(s) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast

groups configured on the Switch. The user may set an IPv4 Multicast address or range of IPv4 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Multicast Profile Settings**, as show below:

Figure 113: IPv4 Multicast Profile Settings window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a Profile ID between *1* and *24*.
Profile Name	Enter a name for the IP Multicast Profile.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

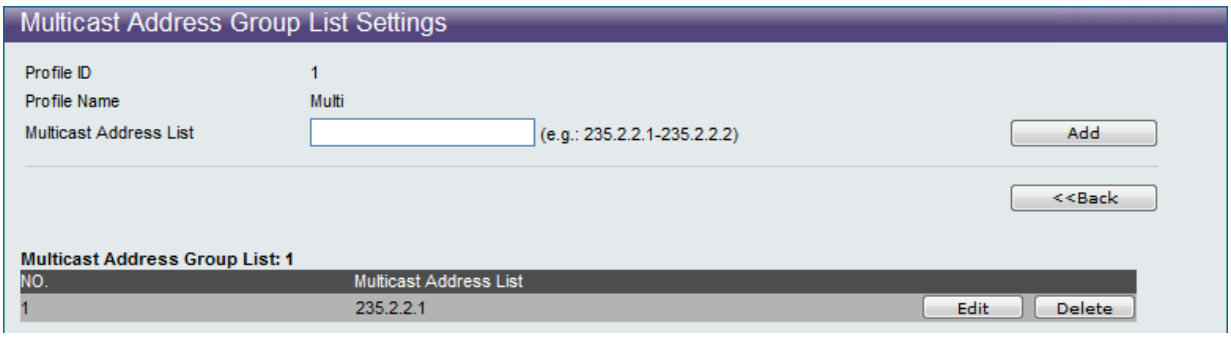
Click the **Group List** link to configure the multicast address group list settings for the specific entry.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Group List** link, the following page will appear:

Figure 114: Multicast Address Group List Settings window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Display the profile ID.
Profile Name	Display the profile name.
Multicast Address List	Enter the multicast address list here.

Click the **Add** button to add a new entry based on the information entered.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Edit** button to re-configure the specific entry.

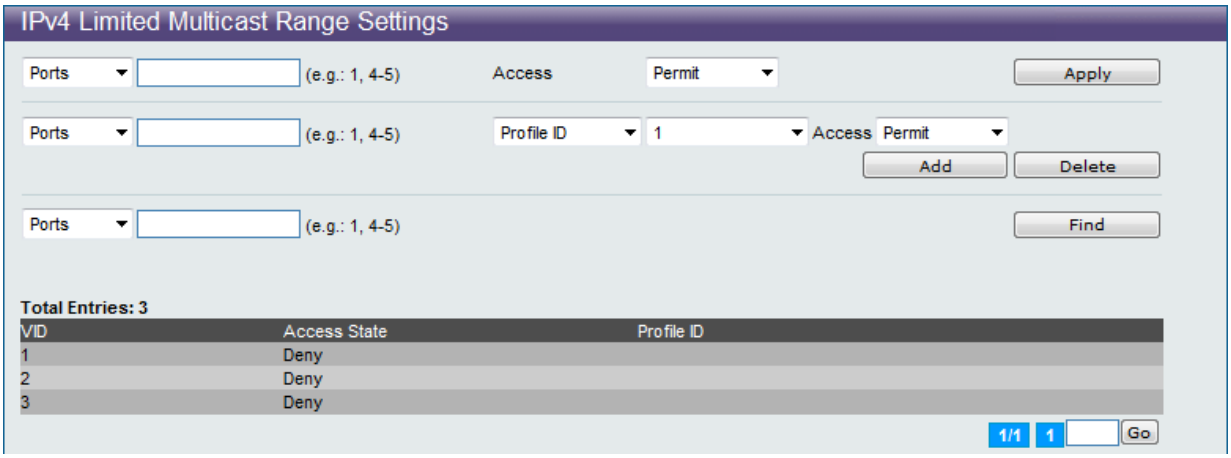
Click the **Delete** button to remove the specific entry.

IPv4 Limited Multicast Range Settings

Users can configure the ports and VLANs on the Switch that will be involved in the Limited IPv4 Multicast Range. The user can configure the range of multicast ports that will be accepted by the source ports to be forwarded to the receiver ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Limited Multicast Range Settings**, as show below:

Figure 115: IPv4 Limited Multicast Range Settings window



The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration.
Access	Assign access permissions to the ports selected. Options listed are **Permit** and **Deny**.
Profile ID / Profile Name:	Use the drop-down menu to select the profile ID or profile name used and then assign **Permit** or **Deny** access to them.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry.

Click the **Find** button to locate a specific entry based on the information entered.

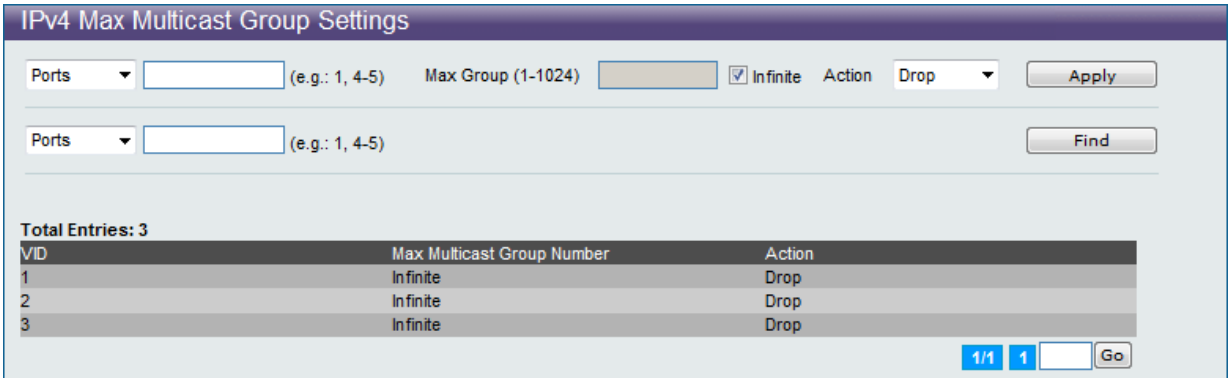
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv4 Max Multicast Group Settings

Users can configure the ports and VLANs on the switch that will be a part of the maximum filter group, up to a maximum of 1024.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Max Multicast Group Settings**, as show below:

Figure 116: IPv4 Max Multicast Group Settings window



The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration here.
Max Group	If the checkbox **Infinite** is not selected, the user can enter a **Max Group** value.
Infinite	Tick the check box to enable or disable the use of the Infinite value.
Action	Use the drop-down menu to select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

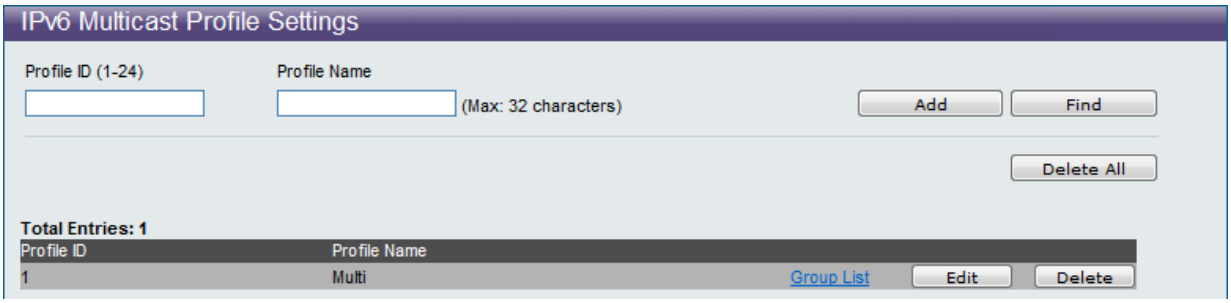
IPv6 Multicast Filtering

IPv6 Multicast Profile Settings

Users can add a profile to which multicast address(s) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IPv6 Multicast address or range of IPv6 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Multicast Profile Settings**, as show below:

Figure 117: IPv6 Multicast Profile Settings window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a Profile ID between *1* and *24*.
Profile Name	Enter a name for the IP Multicast Profile.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

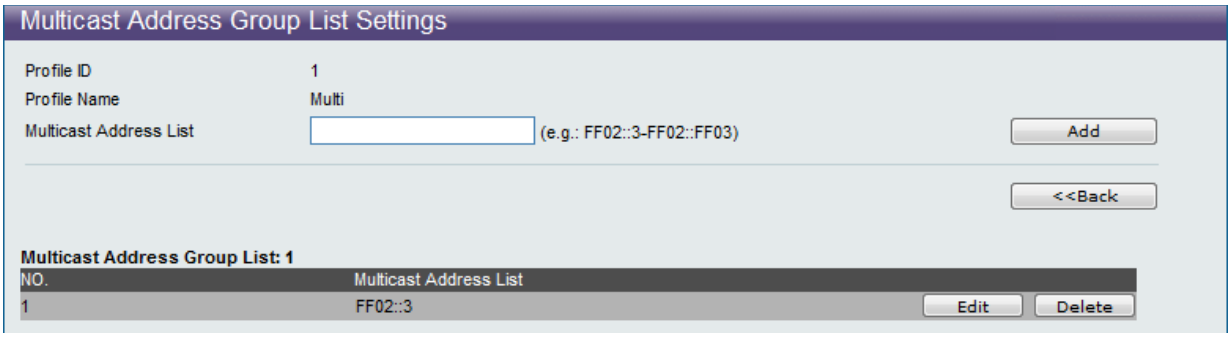
Click the **Group List** link to configure the multicast address group list settings for the specific entry.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:

Figure 118: Multicast Address Group List Settings window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Display the profile ID.
Profile Name	Display the profile name.
Multicast Address List	Enter the multicast address list here.

Click the **Add** button to add a new entry based on the information entered.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Edit** button to re-configure the specific entry.

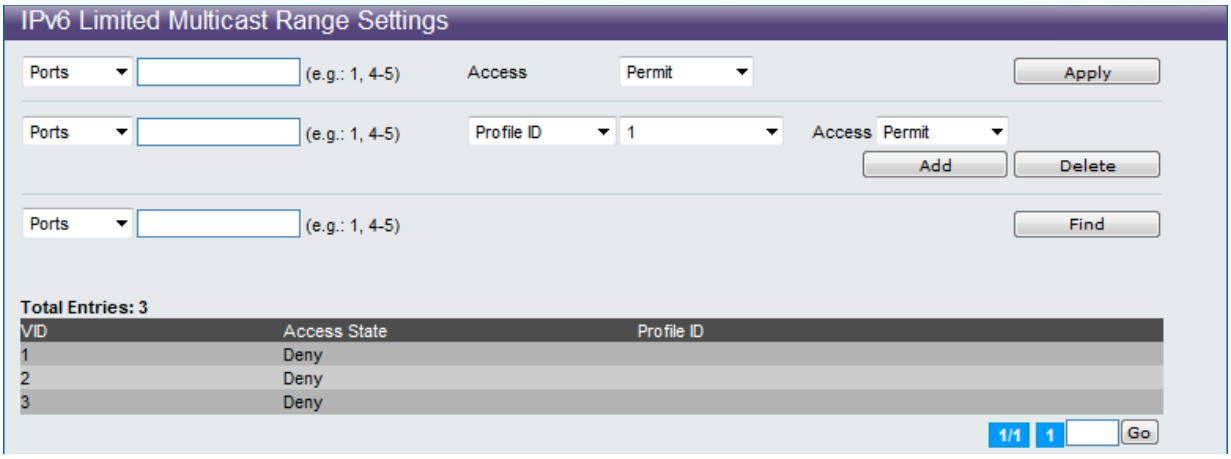
Click the **Delete** button to remove the specific entry.

IPv6 Limited Multicast Range Settings

Users can configure the ports and VLANs on the Switch that will be involved in the Limited IPv6 Multicast Range. The user can configure the range of multicast ports that will be accepted by the source ports to be forwarded to the receiver ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Limited Multicast Range Settings**, as show below:

Figure 119: IPv6 Limited Multicast Range Settings window



The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration.
Access	Assign access permissions to the ports selected. Options listed are **Permit** and **Deny**.
Profile ID / Profile Name:	Use the drop-down menu to select the profile ID or profile name used and then assign **Permit** or **Deny** access to them.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry.

Click the **Find** button to locate a specific entry based on the information entered.

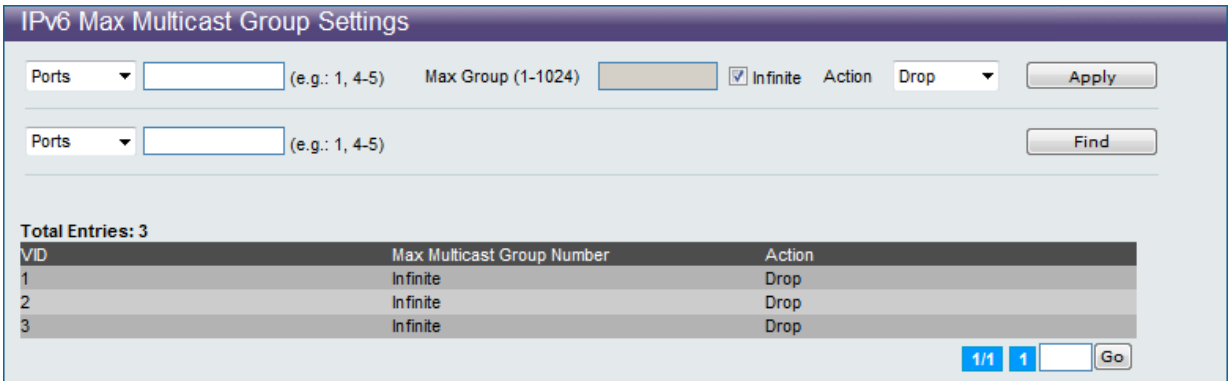
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Max Multicast Group Settings

Users can configure the ports and VLANs on the switch that will be a part of the maximum filter group, up to a maximum of 1024.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Max Multicast Group Settings**, as show below:

Figure 120: IPv6 Max Multicast Group Settings window



The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration here.
Max Group	If the checkbox **Infinite** is not selected, the user can enter a **Max Group** value.
Infinite	Tick the check box to enable or disable the use of the Infinite value.
Action	Use the drop-down menu to select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

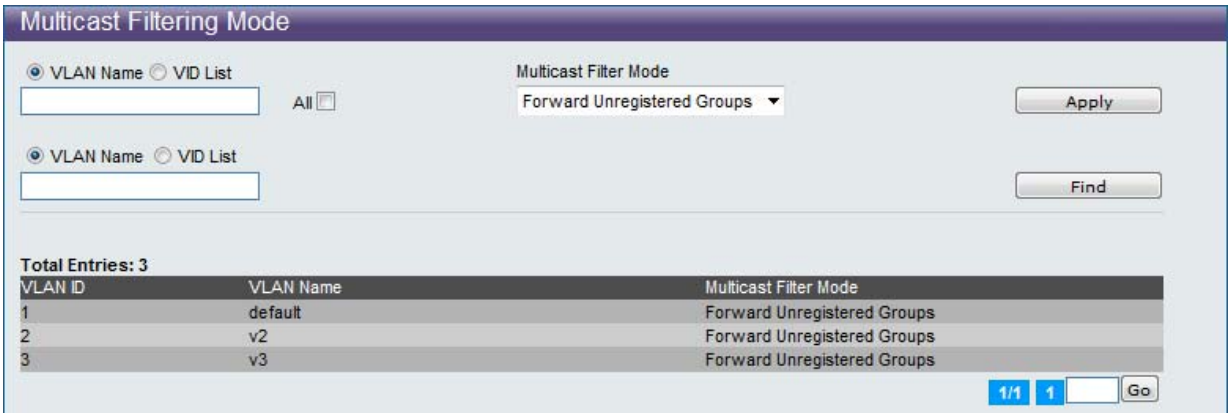
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast Filtering Mode

Users can configure the multicast filtering mode.

To view the following window, click **L2 Features > Multicast Filtering > Multicast Filtering Mode**, as show below:

Figure 121: Multicast Filtering Mode window



The fields that can be configured are described below:

Parameter	Description
VLAN Name/VID List	The VLAN to which the specified filtering action applies. Tick the **All** check box to apply this feature to all the VLANs.
Multicast Filtering Mode	This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that requires forwarding to a port in the specified VLAN. *Forward All Groups* – This will instruct the Switch to forward all multicast packets to the specified VLAN. *Forward Unregistered Groups* – The multicast packets whose destination is an unregistered multicast group will be forwarded within the range of ports specified above. *Filter Unregistered Groups* – The multicast packets whose destination is a registered multicast group will be forwarded within the range of ports specified above.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

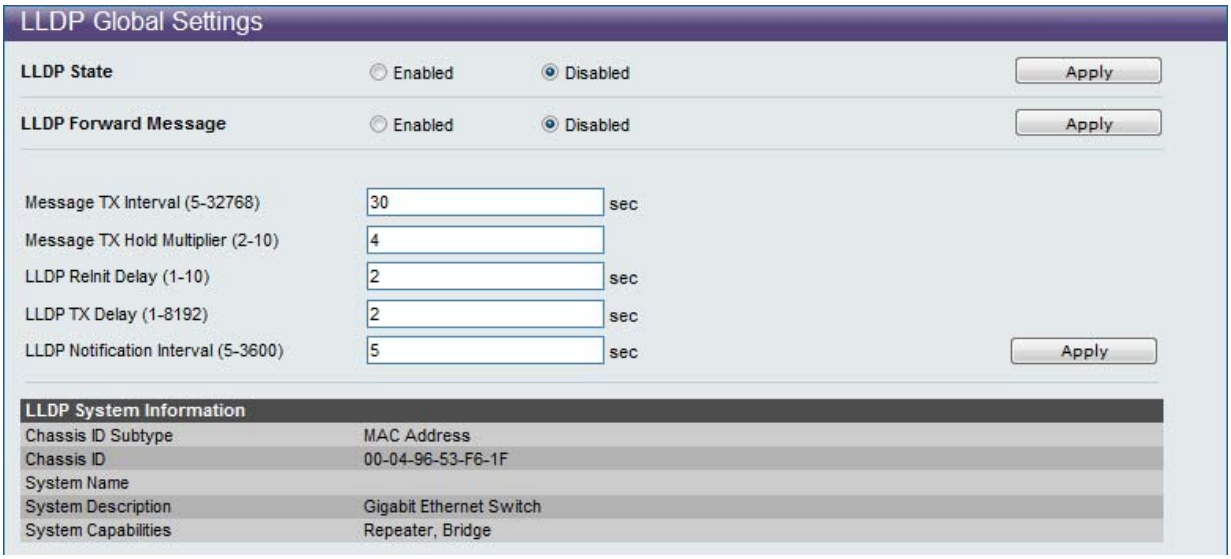
LLDP

LLDP Global Settings

On this page the user can configure the LLDP global parameters.

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as show below:

Figure 122: LLDP Global Settings window



The fields that can be configured are described below:

Parameter	Description
LLDP State	Click the radio buttons to enable or disable the LLDP feature.
LLDP Forward Message	When LLDP is disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message TX Interval	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (5 to 32768).
Message TX Hold Multiplier	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP ReInit Delay	The LLDP re-initialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP re-init delay, enter a value in seconds (1 to 10).
LLDP TX Delay	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (1 to 8192).
LLDP Notification interval	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (5 to 3600).

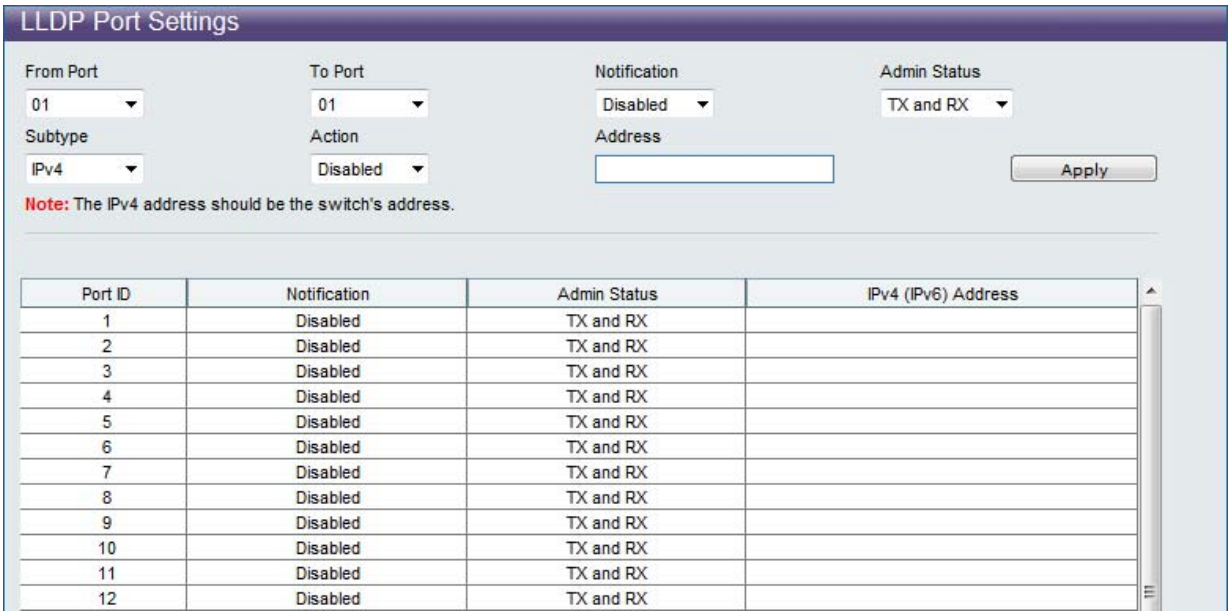
Click the **Apply** button to accept the changes made for each individual section.

LLDP Port Settings

On this page the user can configure the LLDP port parameters.

To view the following window, click **L2 Features > LLDP > LLDP Port Settings**, as show below:

Figure 123: LLDP Port Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select the ports used for this configuration.
Notification	Use the pull-down menu to enable or disable the status of the LLDP notification. This function controls the SNMP trap however it cannot implement traps on SNMP when the notification is disabled.
Admin Status	This function controls the local LLDP agent and allows it to send and receive LLDP frames on the ports. This option contains **TX**, **RX**, **TX And RX** or **Disabled**. *TX*: the local LLDP agent can only transmit LLDP frames. *RX*: the local LLDP agent can only receive LLDP frames. *TX And RX*: the local LLDP agent can both transmit and receive LLDP frames. *Disabled*: the local LLDP agent can neither transmit nor receive LLDP frames. The default value is TX And RX.
Subtype	Use the drop-down menu to select the type of the IP address information will be sent.
Action	Use the drop-down menu to enable or disable the action field.
Address	Enter the IP address that will be sent.

Click the **Apply** button to accept the changes made.

NOTE

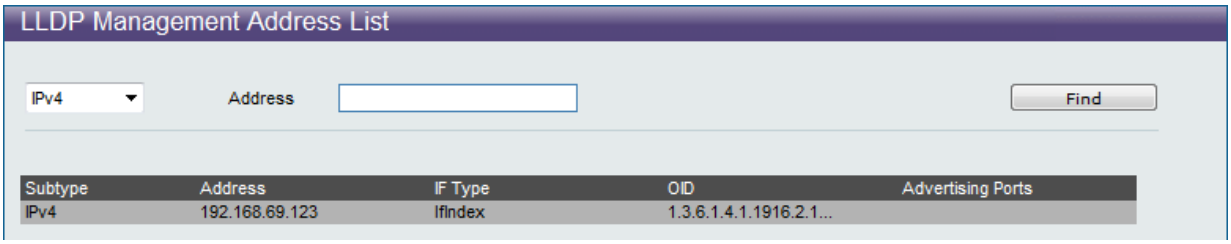
The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

On this page the user can view the LLDP management address list.

To view the following window, click **L2 Features > LLDP > LLDP management Address List**, as show below:

Figure 124: LLDP Management Address List window



The fields that can be configured are described below:

Parameter	Description
IPv4/IPv6	Use the drop-down menu to select either IPv4 or IPv6.
Address	Enter the management IP address or the IP address of the entity you wish to advertise to. The IPv4 address is a management IP address, so the IP information will be sent with the frame.

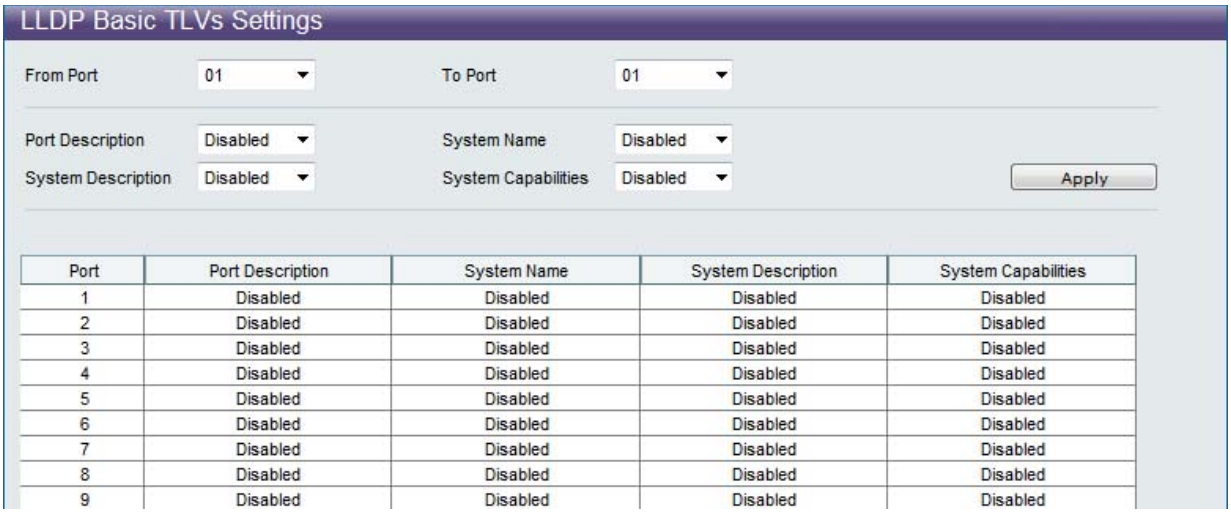
Click the **Find** button to locate a specific entry based on the information entered.

LLDP Basic TLVs Settings

TLV stands for Type-length-value, which allows the specific sending information as a TLV element within LLDP packets. This window is used to enable the settings for the Basic TLVs Settings. An active LLDP port on the Switch always included mandatory data in its outbound advertisements. There are four optional data types that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory data types cannot be disabled. There are also four data types which can be optionally selected. These include Port Description, System Name, System Description and System Capability.

To view the following window, click **L2 Features > LLDP > LLDP Basic TLVs Settings**, as show below:

Figure 125: LLDP Basic TLVs Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the port range to use for this configuration.
Port Description	Use the drop-down menu to enable or disable the Port Description option.
System Name	Use the drop-down menu to enable or disable the System Name option.
System Description	Use the drop-down menu to enable or disable the System Description option.
System Capabilities	Use the drop-down menu to enable or disable the System Capabilities option.

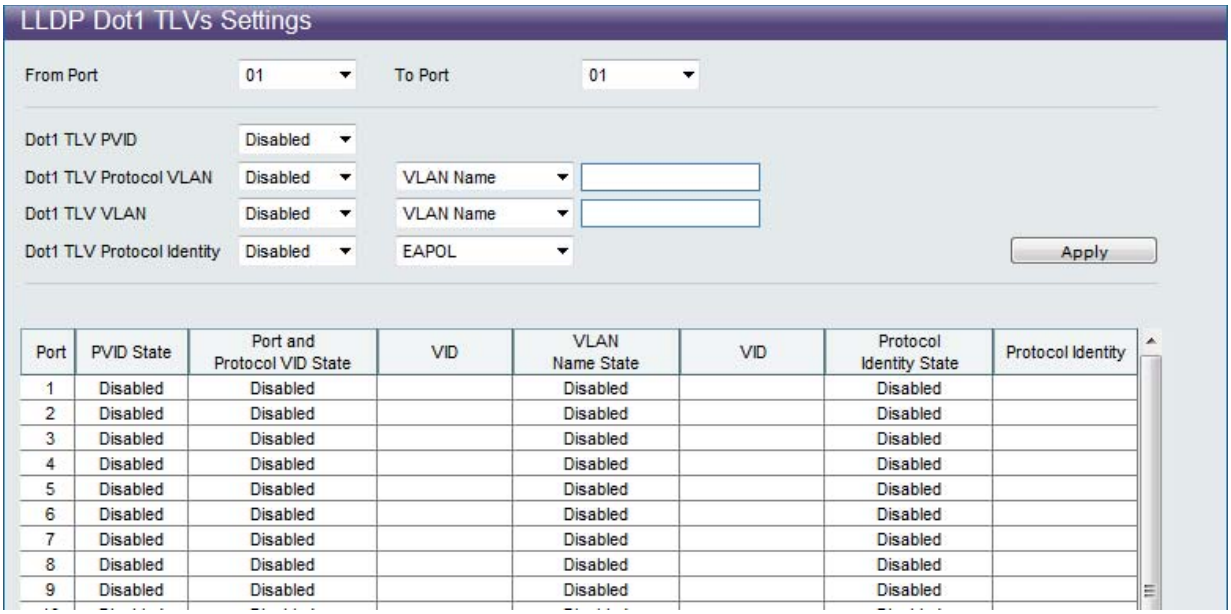
Click the **Apply** button to accept the changes made.

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs which are defined in IEEE 802.1 and used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Dot1 TLVs Settings**, as show below:

Figure 126: LLDP Dot1 TLVs Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
Dot1 TLV PVID	Use the drop-down menu to enable or disable and configure the Dot1 TLV PVID option.
Dot1 TLV Protocol VLAN	Use the drop-down menu to enable or disable, and configure the Dot1 TLV Protocol VLAN option. After enabling this option to the user can select to use either **VLAN Name**, **VID List** or **All** in the next drop-down menu. After selecting this, the user can enter either the **VLAN Name** or **VID List** value in the space provided.
Dot1 TLV VLAN	Use the drop-down menu to enable or disable, and configure the Dot1 TLV VLAN option. After enabling this option to the user can select to use either **VLAN Name**, **VID List** or **All** in the next drop-down menu. After selecting this, the user can enter either the **VLAN Name** or **VID List** value in the space provided.
Dot1 TLV Protocol Identity	Use the drop-down menu to enable or disable, and configure the Dot1 TLV Protocol Identity option. After enabling this option the user can select to either use **EAPOL**, **LACP**, **GVRP**, **STP**, or **All**.

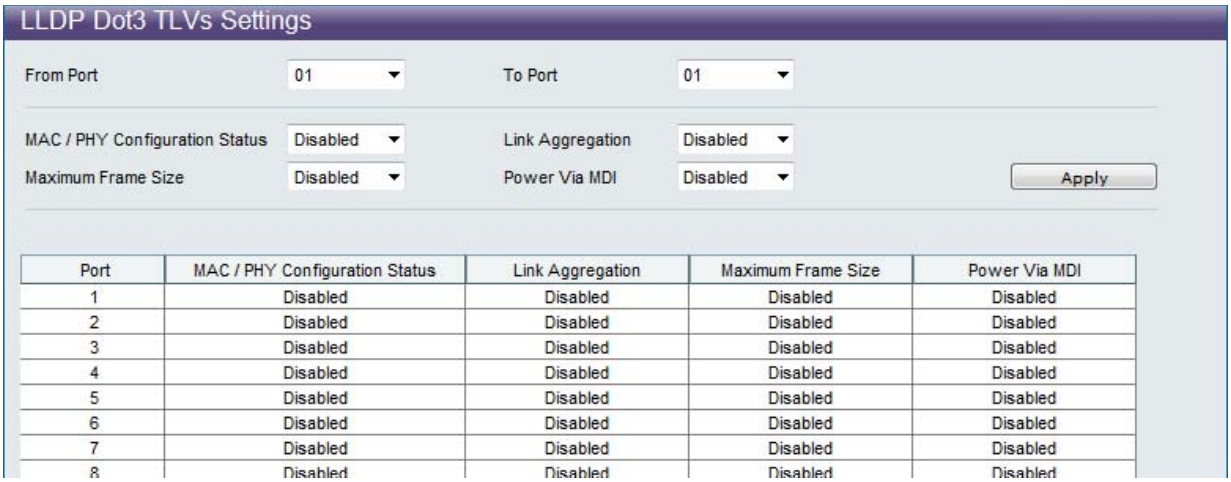
Click the **Apply** button to accept the changes made.

LLDP Dot3 TLVs Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP Dot3 TLVs Settings**, as show below:

Figure 127: LLDP Dot3 TLVs Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
MAC / PHY Configuration Status	This TLV optional data type indicates that the LLDP agent should transmit the MAC/PHY configuration/status TLV. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is Disabled.
Link Aggregation	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is Disabled.
Maximum Frame Size	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is Disabled.

Click the **Apply** button to accept the changes made.

LLDP Statistic System

The LLDP Statistics System page allows you an overview of the neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch. Select a **Port** number from the drop-down menu and click the **Find** button to view statistics for a certain port.

To view the following window, click **L2 Features > LLDP > LLDP Statistic System**, as show below:

Figure 128: LLDP Statistics System window

LLDP Statistics System
LLDP Statistics
Last Change Time 1637
Number of Table Insert 0
Number of Table Delete 0
Number of Table Drop 0
Number of Table Ageout 0
Port 01
Find
LLDP Statistics Ports
Total TX Frames 0
Total Discarded RX Frames 0
RX Errors Frames 0
Total RX Frames 0
Total Discarded RX TLVs 0
Total Unrecognized RX TLVs 0
Total Aged out Neighbor Information 0

LLDP Local Port Information

The LLDP Local Port Information page displays the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

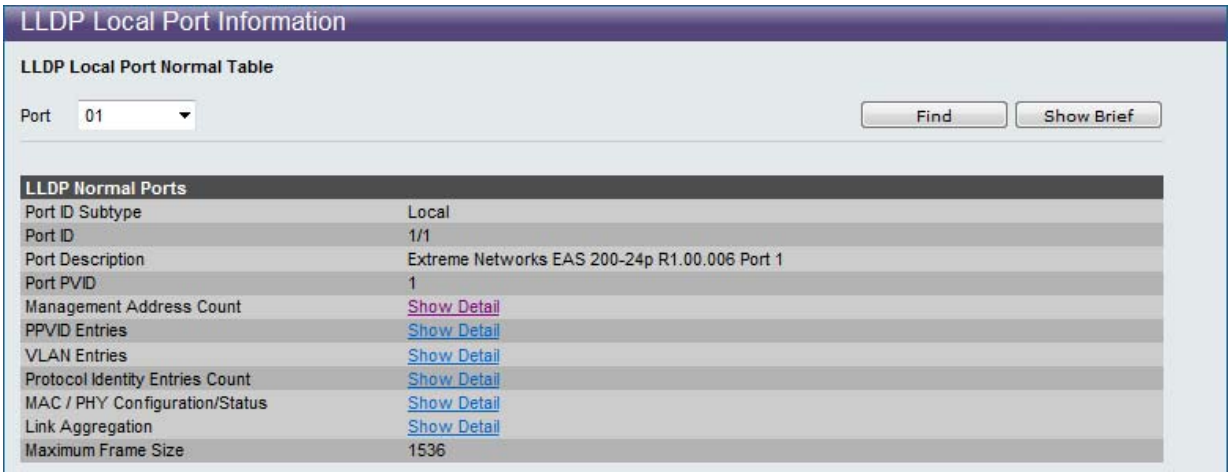
To view the following window, click **L2 Features > LLDP > LLDP Local Port Information**, as show below:

Figure 129: LLDP Local Port Information window

To view the normal LLDP Local Port information page per port, click the **Show Normal** button.

To view the brief LLDP Local Port information page per port, click the **Show Brief** button.

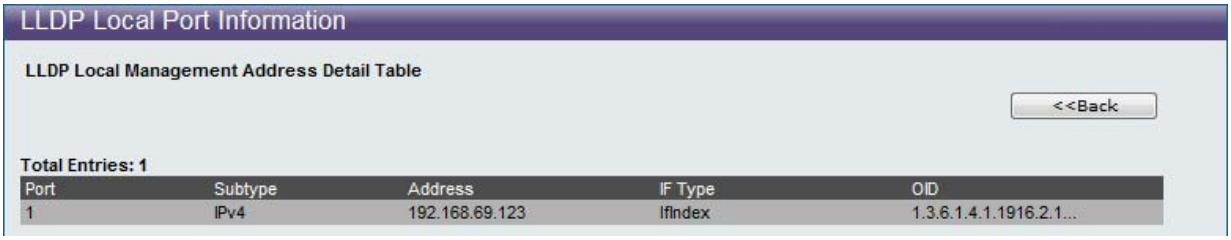
Figure 130: LLDP Local Port Information – Show Normal window


LLDP Local Port Information
LLDP Local Port Normal Table
Port 01
Find
Show Brief
LLDP Normal Ports
Port ID Subtype Local
Port ID 1/1
Port Description Extreme Networks EAS 200-24p R1.00.006 Port 1
Port PVID 1
Management Address Count Show Detail
PPVID Entries Show Detail
VLAN Entries Show Detail
Protocol Identity Entries Count Show Detail
MAC / PHY Configuration/Status Show Detail
Link Aggregation Show Detail
Maximum Frame Size 1536

Select a **Port** number and click the **Find** button to locate a specific entry.

To view more details about, for example, the **Management Address Count**, click on the Show Detail hyperlink.

Figure 131: LLDP Local Port Information – Show Detail window


LLDP Local Port Information
LLDP Local Management Address Detail Table
<<Back
Total Entries: 1
Port Subtype Address IF Type OID
1 IPv4 192.168.69.123 IfIndex 1.3.6.1.4.1.1916.2.1...

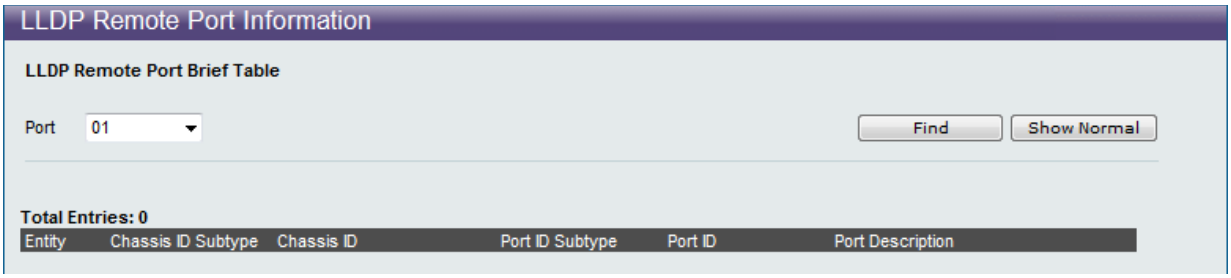
Click the **<<Back** button to return to the previous page.

LLDP Remote Port Information

This page displays port information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

To view the following window, click **L2 Features > LLDP > LLDP Remote Port Information**, as show below:

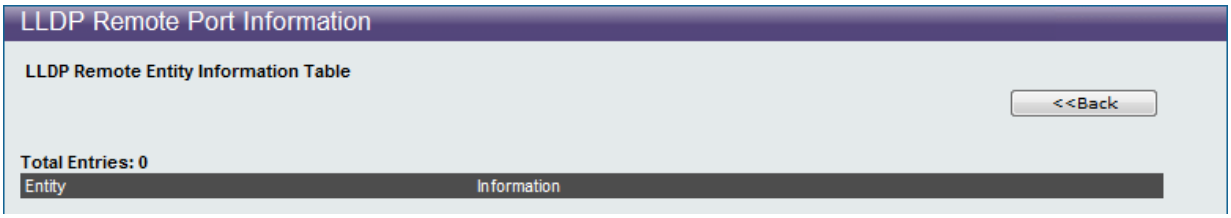
Figure 132: LLDP Remote Port Information window



Select a **Port** number and click the **Find** button to locate a specific entry.

To view the normal LLDP Remote Port information page per port, click the **Show Normal** button.

Figure 133: LLDP Remote Port Information – Show Normal window



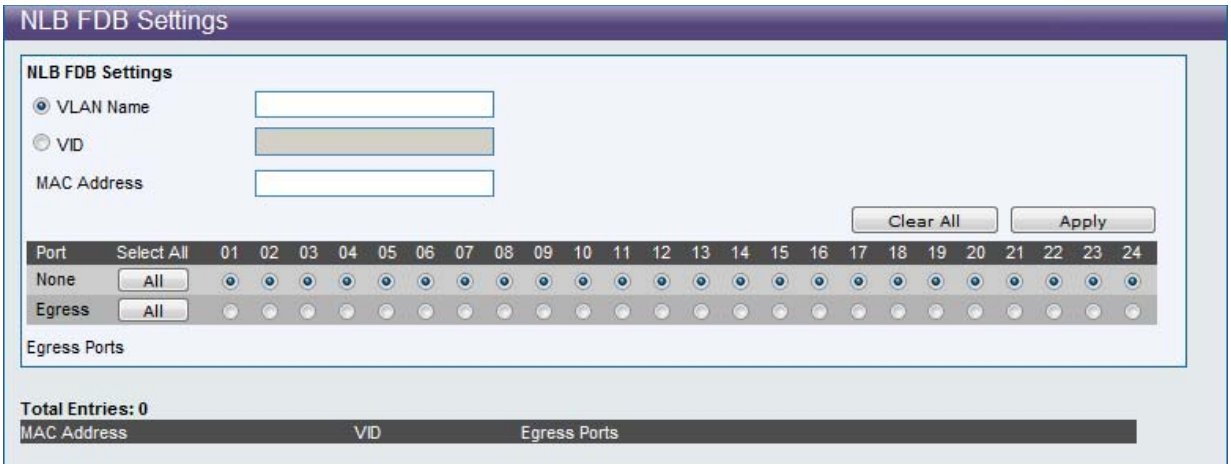
Click the **<<Back** button to return to the previous page.

NLB FDB Settings

The Switch supports Network Load Balancing (NLB). This is a MAC forwarding control for supporting the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. In multicast mode, the client uses a multicast MAC address as the destination MAC to reach the server. Regardless of the mode, the destination MAC is the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet. The NLB multicast FDB entry will be mutually exclusive with the L2 multicast entry.

To view this window, click **L2 Features > NLB FDB Settings**, as shown below.

Figure 134: NLB Multicast FDB Table window



The following fields can be set:

Parameter	Description
VLAN Name	Click the radio button and enter the VLAN of the NLB multicast FDB entry to be created.
VID (1-4094)	Click the radio button and enter the VLAN by the VLAN ID.
MAC Address	Enter the MAC address of the NLB multicast FDB entry to be created.

Click the **Apply** button to accept the changes made.

Click the **Clear All** button to remove all the entered information in the fields.

Click the **Edit** button to update the information of the corresponding entry.

Click the **Delete** button to delete the corresponding entry.

5 L3 Features

CHAPTER

IPv4 Static/Default Route Settings

The Switch supports static routing for IPv4 formatted addressing. Users can create up to 512 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP response will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become Active.

Entries into the Switch's forwarding table can be made using both an IP address subnet mask and a gateway.

To view the following window, click **L3 Features > IPv4 Static/Default Route Settings**, as show below:

Figure 135: IPv4 Static/Default Route Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	This field allows the entry of an IPv4 address to be assigned to the Static or Default route.

Parameter	Description
Netmask	This field allows the entry of a subnet mask to be applied to the corresponding subnet mask of the IP address.
Gateway	This field allows the entry of a Gateway IP Address to be applied to the corresponding gateway of the IP address.
Metric	Represents the metric value of the IP interface entered into the table. This field may read a number between 1 and 65535.
Backup State	Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, switch will try the backup routes according to the order learnt by the routing table until route success. The field represents the Backup state that the Static and Default Route is configured for.

Click the **Apply** button to accept the changes made.

IPv4 Route Table

The IP routing table stores all the external routes information of the switch. On this page the user can view all the external route information on the switch.

To view the following window, click **L3 Features > IPv4 Route Table**, as show below:

Figure 136: IPv4 Route Table window

IPv6 Static/Default Route Settings

A static entry of an IPv6 address can be entered into the Switch's routing table for IPv6 formatted addresses.

To view the following window, click **L3 Features > IPv6 Static/Default Route Settings**, as show below:

Figure 137: IPv6 Static/Default Route Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	The IP Interface where the static IPv6 route is created.
Nexthop Address	The corresponding IPv6 address for the next hop Gateway address in IPv6 format.
Metric	The metric of the IPv6 interface entered into the table representing the number of routers between the Switch and the IPv6 address above. Metric values allowed are between 1 and 65535.
Backup State	Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, the switch will try the backup routes according to the order learnt by the routing table until route success. This field represents the backup state for the IPv6 configured. This field may be Primary or Backup.

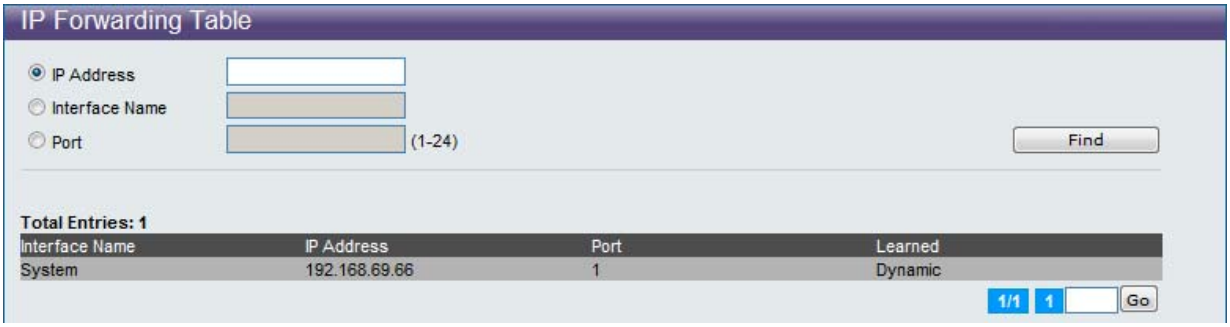
Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

IP Forwarding Table

The IP forwarding table stores all the direct connected IP information. On this page the user can view all the direct connected IP information. To view the following window, click **L3 Features > IP Forwarding Table**, as show below:

Figure 138: IP Forwarding Table



Click the **IP Address**, **Interface Name** or **Port** radio button, enter the information and click the **Find** button to locate a specific entry based on the information entered. Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

6 QoS

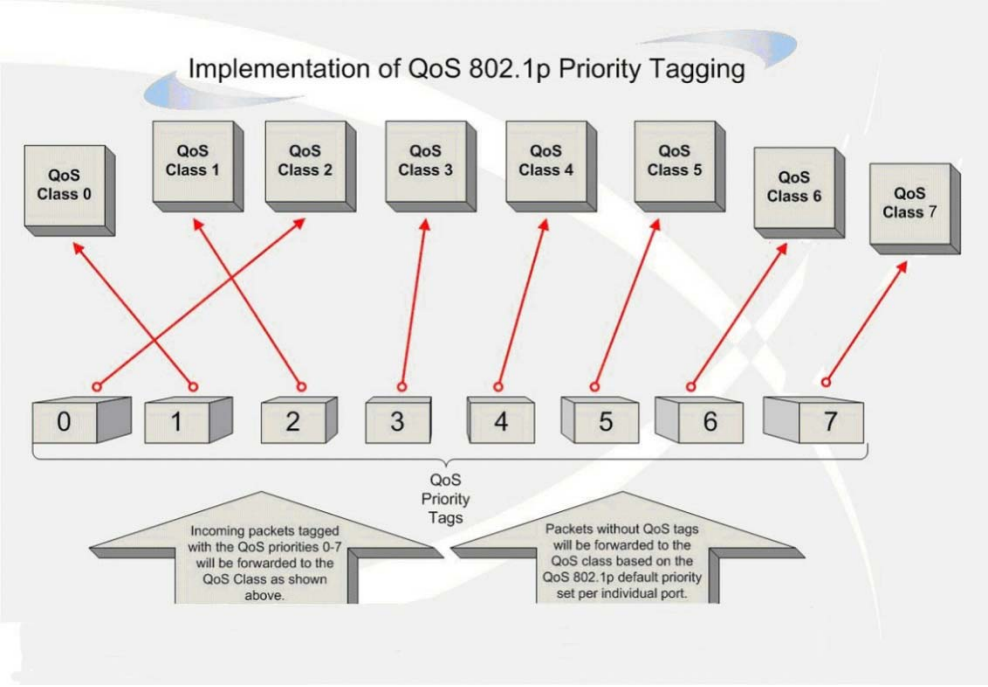
CHAPTER

The Switch supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements basic 802.1P priority queuing.

Figure 139: Mapping QoS on the Switch


Implementation of QoS 802.1p Priority Tagging
QoS Class 0
QoS Class 1
QoS Class 2
QoS Class 3
QoS Class 4
QoS Class 5
QoS Class 6
QoS Class 7
0
1
2
3
4
5
6
7
QoS Priority Tags
Incoming packets tagged with the QoS priorities 0-7 will be forwarded to the QoS Class as shown above.
Packets without QoS tags will be forwarded to the QoS class based on the QoS 802.1p default priority set per individual port.

The picture above shows the default priority setting for the Switch. Class-7 has the highest priority of the seven priority classes of service on the Switch. In order to implement QoS, the user is required to

instruct the Switch to examine the header of a packet to see if it has the proper identifying tag. Then the user may forward these tagged packets to designated classes of service on the Switch where they will be emptied, based on priority.

For example, let's say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch supports 802.1p priority queuing. The Switch has eight priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

For strict priority-based scheduling, any packets residing in the higher priority classes of service are transmitted first. Multiple strict priority classes of service are emptied based on their priority tags. Only when these classes are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of eight CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the Switch has eight configurable priority queues (and eight Classes of Service) for each port on the Switch.

CAUTION

The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and is therefore not configurable. All references in the following section regarding classes of service will refer to only the eight classes of service that may be used and configured by the administrator.

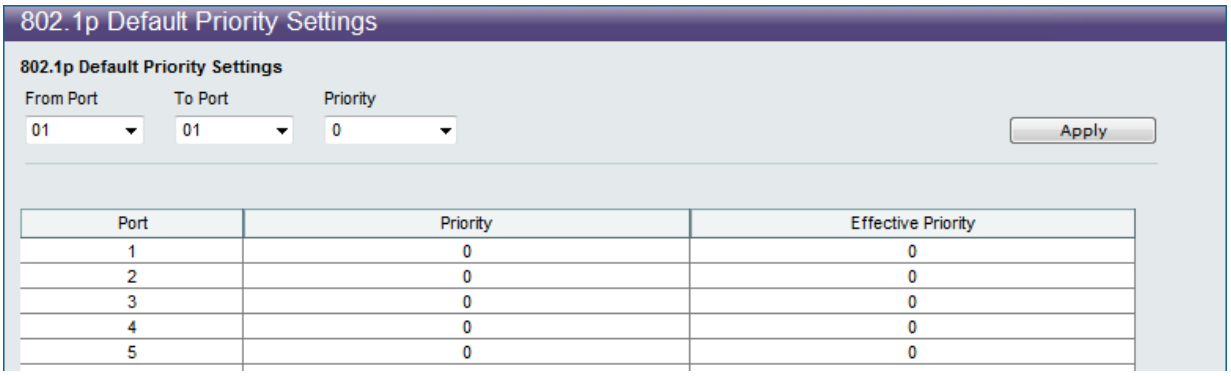
802.1p Settings

802.1p Default Priority Settings

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. This page allows the user to assign a default 802.1p priority to any given port on the switch that will insert the 802.1p priority tag to untagged packets received. The priority and effective priority tags are numbered from *0*, the lowest priority, to *7*, the highest priority. The effective priority indicates the actual priority assigned by RADIUS. If the RADIUS assigned value exceeds the specified limit, the value will be set at the default priority. For example, if the RADIUS assigns a limit of 8 and the default priority is 0, the effective priority will be 0.

To view the following window, click **QoS > 802.1p Settings > 802.1p Default Priority Settings**, as show below:

Figure 140: Default Priority Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the starting and ending ports to use.
Priority	Use the drop-down menu to select a value from *0* to *7*.

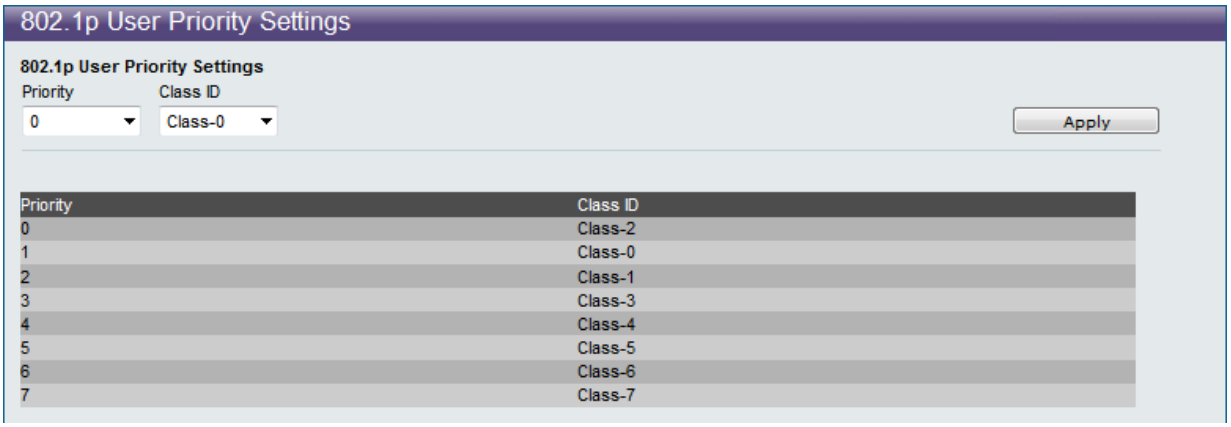
Click the **Apply** button to accept the changes made.

802.1p User Priority Settings

The Switch allows the assignment of a class of service to each of the 802.1p priorities.

To view the following window, click **QoS > 802.1p Settings > 802.1p User Priority Settings**, as show below:

Figure 141: 802.1p User Priority Settings window



Once a priority has been assigned to the port groups on the Switch, then a Class may be assigned to each of the eight levels of 802.1p priorities using the drop-down menus on this window. User priority mapping is not only for the default priority configured in the last page, but also for all the incoming tagged packets with 802.1p tag.

Click the **Apply** button to accept the changes made.

Bandwidth Control

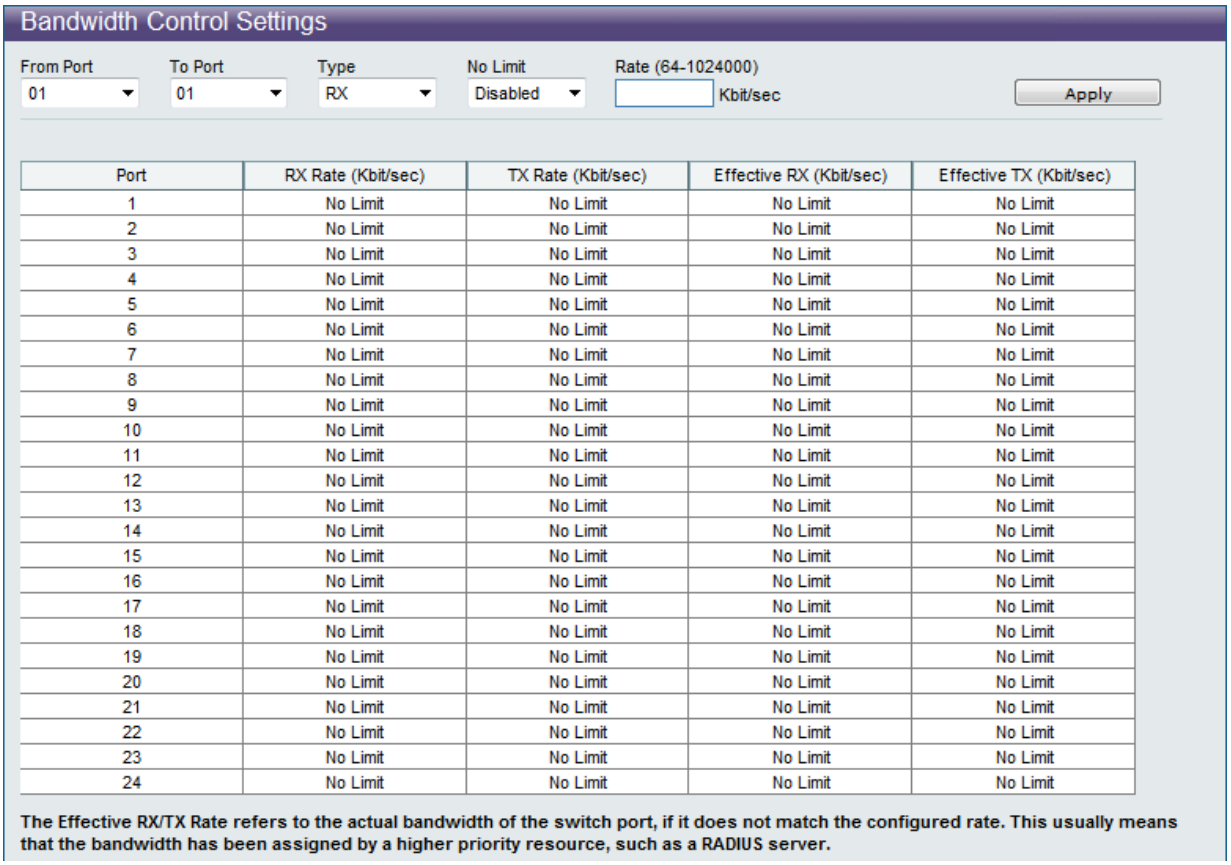
The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

Bandwidth Control Settings

The Effective RX/TX Rate refers to the actual bandwidth of the switch port, if it does not match the configured rate. This usually means that the bandwidth has been assigned by a higher priority resource, such as a RADIUS server.

To view the following window, click **QoS > Bandwidth Control > Bandwidth Control Settings**, as show below:

Figure 142: Bandwidth Control Settings window


Bandwidth Control Settings
From Port
01
To Port
01
Type
RX
No Limit
Disabled
Rate (64-1024000)
Kbit/sec
Apply
Port
RX Rate (Kbit/sec)
TX Rate (Kbit/sec)
Effective RX (Kbit/sec)
Effective TX (Kbit/sec)
1 No Limit No Limit No Limit No Limit
2 No Limit No Limit No Limit No Limit
3 No Limit No Limit No Limit No Limit
4 No Limit No Limit No Limit No Limit
5 No Limit No Limit No Limit No Limit
6 No Limit No Limit No Limit No Limit
7 No Limit No Limit No Limit No Limit
8 No Limit No Limit No Limit No Limit
9 No Limit No Limit No Limit No Limit
10 No Limit No Limit No Limit No Limit
11 No Limit No Limit No Limit No Limit
12 No Limit No Limit No Limit No Limit
13 No Limit No Limit No Limit No Limit
14 No Limit No Limit No Limit No Limit
15 No Limit No Limit No Limit No Limit
16 No Limit No Limit No Limit No Limit
17 No Limit No Limit No Limit No Limit
18 No Limit No Limit No Limit No Limit
19 No Limit No Limit No Limit No Limit
20 No Limit No Limit No Limit No Limit
21 No Limit No Limit No Limit No Limit
22 No Limit No Limit No Limit No Limit
23 No Limit No Limit No Limit No Limit
24 No Limit No Limit No Limit No Limit
The Effective RX/TX Rate refers to the actual bandwidth of the switch port, if it does not match the configured rate. This usually means that the bandwidth has been assigned by a higher priority resource, such as a RADIUS server.

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
Type	This drop-down menu allows a selection between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	This drop-down menu allows the user to specify that the selected port will have no bandwidth limit or not. **NOTE:** If the configured number is larger than the port speed, it means no bandwidth limit.
Rate (64-1024000)	This field allows the input of the data rate that will be the limit for the selected port. The user may choose a rate between *64* and *1024000* Kbits per second.
Effective RX	If a RADIUS server has assigned the RX bandwidth, then it will be the effective RX bandwidth. The authentication with the RADIUS sever can be per port or per user. For per user authentication, there may be multiple RX bandwidths assigned if there are multiple users attached to this specific port. The final RX bandwidth will be the largest one among these multiple RX bandwidths.

Parameter	Description
Effective TX	If a RADIUS server has assigned the TX bandwidth, then it will be the effective TX bandwidth. The authentication with the RADIUS sever can be per port or per user. For per user authentication, there may be multiple TX bandwidths assigned if there are multiple users attached to this specific port. The final TX bandwidth will be the largest one among these multiple TX bandwidths.

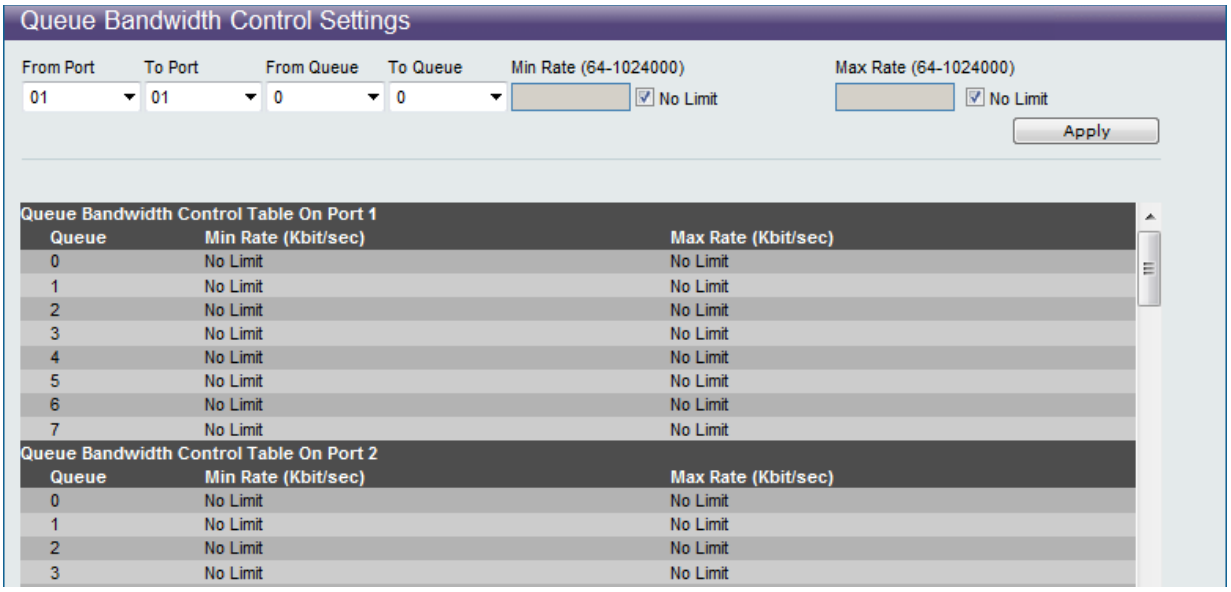
Click the **Apply** button to accept the changes made.

Queue Bandwidth Control Settings

To view this window, click **QoS > Bandwidth Control > Queue Bandwidth Control Settings**, as shown below.

To view the following window, click **QoS > Bandwidth Control > Queue Bandwidth Control Settings**, as show below:

Figure 143: Queue Bandwidth Control Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
From Queue / To Queue	Use the drop-down menu to select the queue range to use for this configuration.
Min Rate	Specify the packet limit, in Kbps that the ports are allowed to receive. Tick the **No limit** check box to have unlimited rate of packets received by the specified queue.
Max Rate	Enter the maximum rate for the queue. For no limit select the **No Limit** option.

Click the **Apply** button to accept the changes made.

NOTE

The minimum granularity of queue bandwidth control is 64Kbit/sec. The system will adjust the number to the multiple of 64 automatically.

Traffic Control Settings

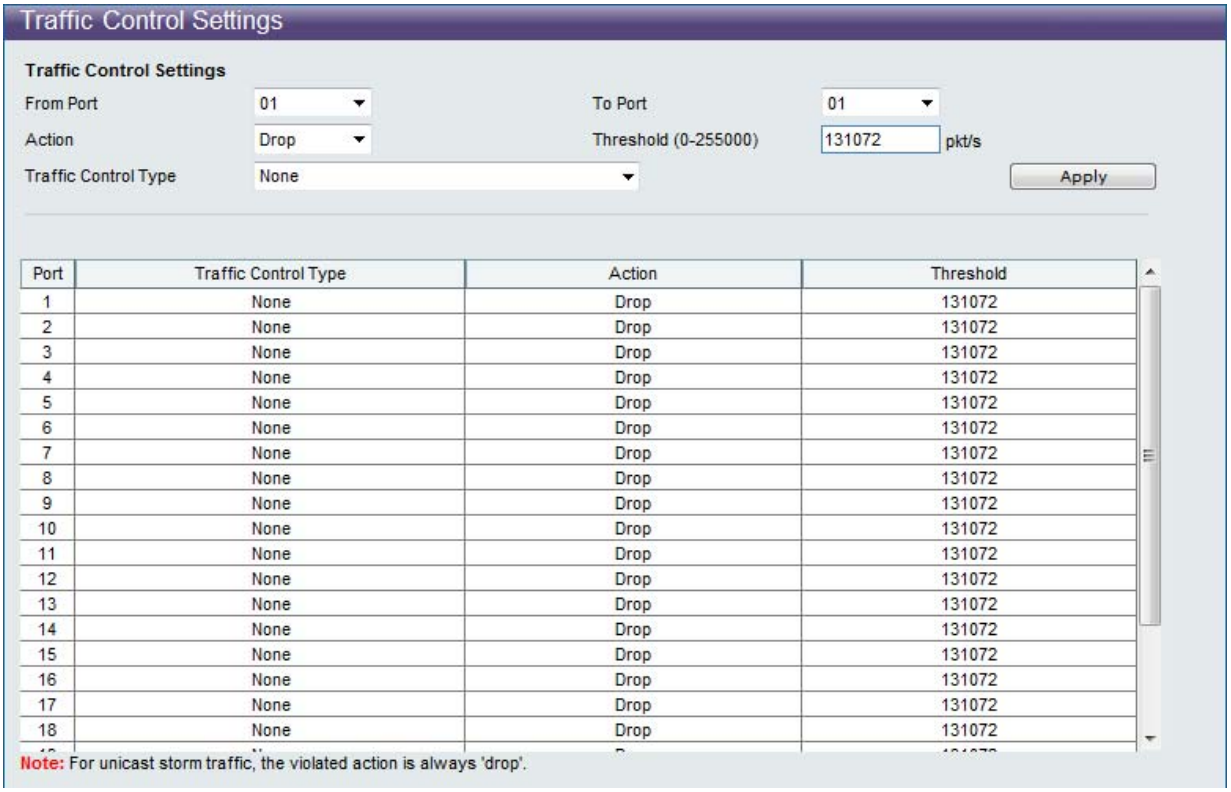
On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious end station on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

Packet storms are monitored to determine if too many packets are flooding the network based on threshold levels provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the *Drop* option of the Action parameter in the window below.

Use this window to enable or disable storm control and adjust the threshold for multicast and broadcast storms.

To view the following window, click **QoS > Traffic Control Settings**, as show below:

Figure 144: Traffic Control Settings window


Traffic Control Settings
Traffic Control Settings
From Port 01
To Port 01
Action Drop
Threshold (0-255000) 131072 pkt/s
Traffic Control Type None
Apply
Port | Traffic Control Type | Action | Threshold
1 None Drop 131072
2 None Drop 131072
3 None Drop 131072
4 None Drop 131072
5 None Drop 131072
6 None Drop 131072
7 None Drop 131072
8 None Drop 131072
9 None Drop 131072
10 None Drop 131072
11 None Drop 131072
12 None Drop 131072
13 None Drop 131072
14 None Drop 131072
15 None Drop 131072
16 None Drop 131072
17 None Drop 131072
18 None Drop 131072
Note: For unicast storm traffic, the violated action is always 'drop'.

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
Action	Select the method of traffic control from the pull-down menu. The choices are: *Drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.
Threshold (0-255000)	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from *0-255000* with a default setting of *131072* packets per second.
Traffic Control Type	Specifies the desired Storm Control Type: *None*, *Broadcast*, *Multicast*, *Unknown Unicast*, *Broadcast + Multicast*, *Broadcast + Unknown Unicast*, *Multicast + Unknown Unicast*, and *Broadcast + Multicast + Unknown Unicast*.

Click the **Apply** button to accept the changes made for each individual section.

NOTE

Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).

NOTE

The minimum granularity of storm control on a GE port is 1pps

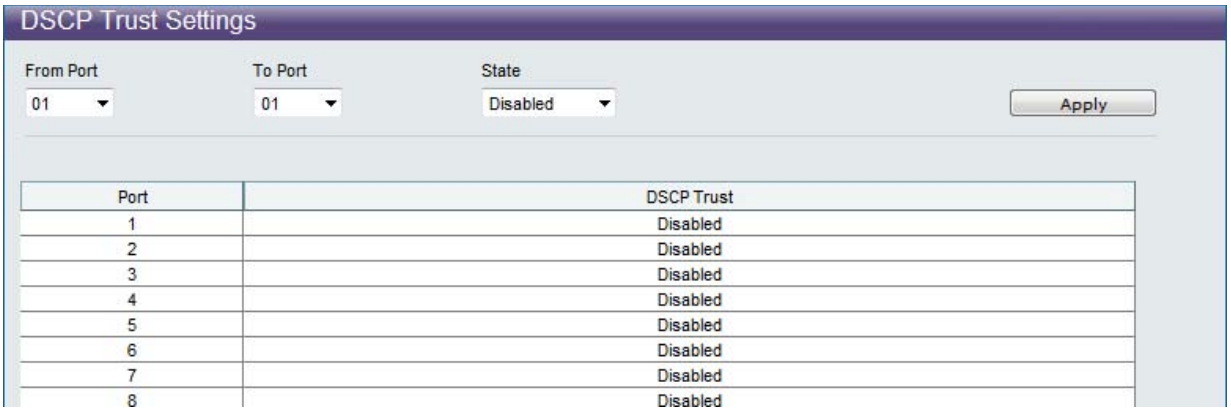
DSCP

DSCP Trust Settings

This page is to configure the DSCP trust state of ports. When ports are under the DSCP trust mode, the switch will insert the priority tag to untagged packets by using the DSCP Map settings instead of the default port priority.

To view the following window, click **QoS > DSCP > DSCP Trust Settings**, as show below:

Figure 145: DSCP Trust Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select a range of port to configure.
State	Enable/disable to trust DSCP. By default, DSCP trust is disabled.

Click the **Apply** button to accept the changes made.

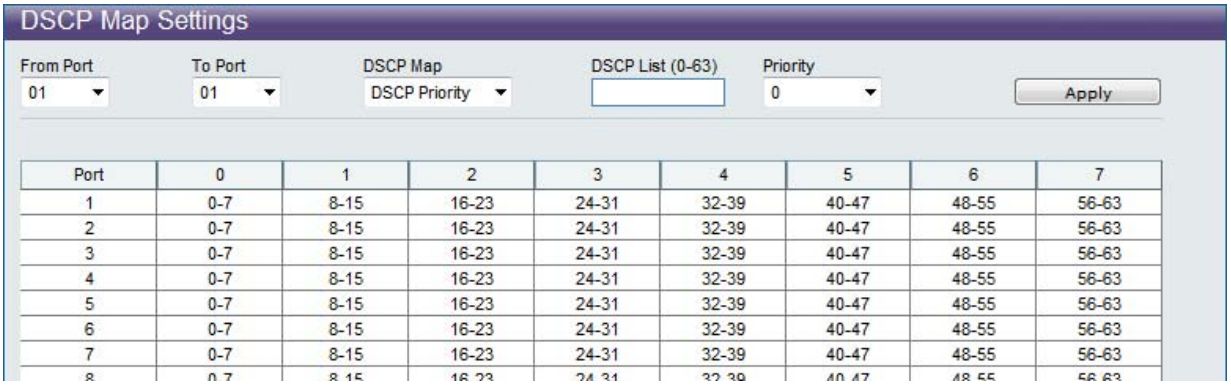
DSCP Map Settings

The mapping of DSCP to queue will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

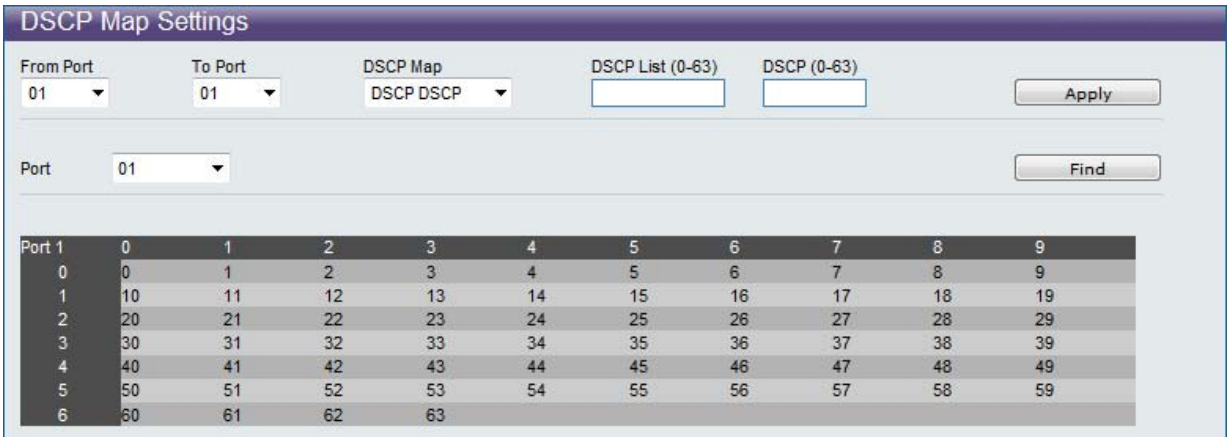
To view the following window, click **QoS > DSCP > DSCP Map Settings**, as show below:

Figure 146: DSCP Map Settings - DSCP Priority window



To view the following window, click **QoS > DSCP > DSCP Map Settings** and select **DSCP DSCP** from the **DSCP Map** drop-down menu, as show below:

Figure 147: DSCP Map Settings - DSCP DSCP window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menu to select a range of port to configure.
DSCP Map	Use the drop-down menu to select one of two options: *DSCP Priority* – Specifies a list of DSCP values to be mapped to a specific priority. *DSCP DSCP* – Specifies a list of DSCP value to be mapped to a specific DSCP.
DSCP List	Enter a DSCP List value.
Priority	Use the drop-down menu to select a Priority value. This appears when selecting **DSCP Priority** in the **DSCP Map** drop-down menu.
DSCP	Enter a DSCP value. This appears when selecting **DSCP Priority** in the **DSCP DSCP** drop-down menu.

Click the **Apply** button to accept the changes made.

HOL Blocking Prevention

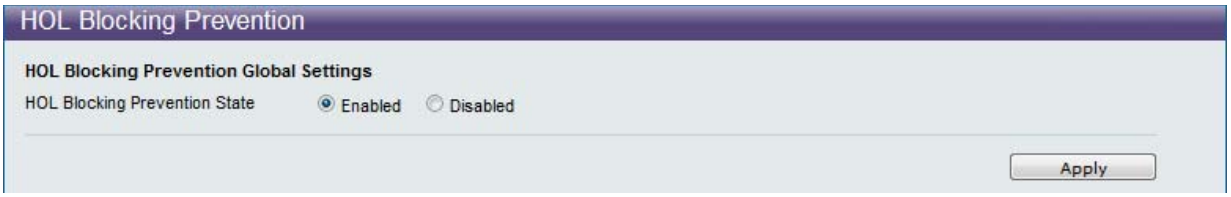
HOL (Head of Line) Blocking happens when one of the destination ports of a broadcast or multicast packet are busy. The switch will hold this packet in the buffer while the other destination port will not transmit the packet even they are not busy.

The HOL Blocking Prevention will ignore the busy port and forward the packet directly to have lower latency and better performance.

On this page the user can enable or disable HOL Blocking Prevention.

To view the following window, click **QoS > HOL Blocking Prevention**, as show below:

Figure 148: HOL blocking Prevention window



The fields that can be configured are described below:

Parameter	Description
HOL Blocking Prevention State	Click the radio buttons to enable of disable the HOL blocking prevention global settings.

Click the **Apply** button to accept the changes made.

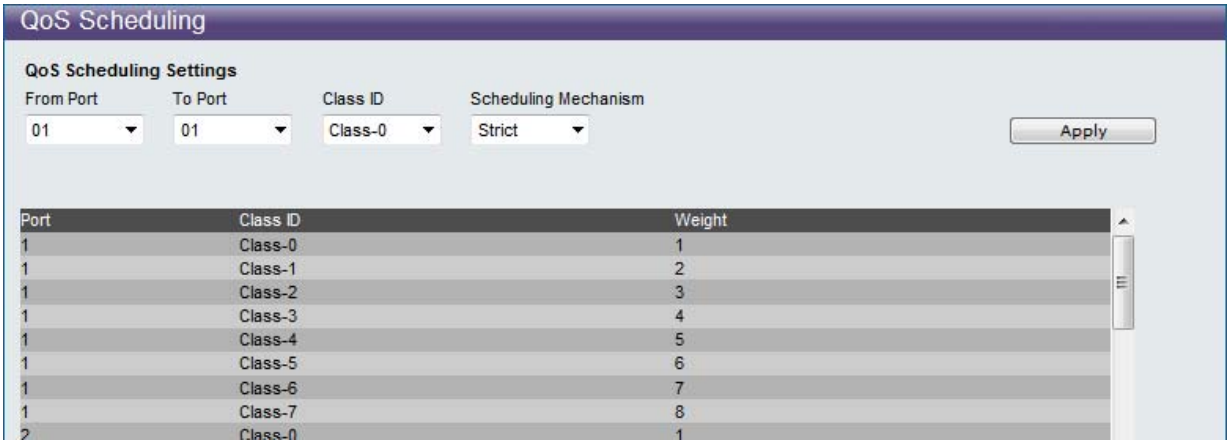
Scheduling Settings

QoS Scheduling

This window allows the user to configure the way the Switch will map an incoming packet per port based on its 802.1p user priority, to one of the eight available hardware priority queues available on the Switch.

To view this window, click **QoS > Scheduling Settings > QoS Scheduling** as shown below:

Figure 149: QoS Scheduling window



The following parameters can be configured:

Parameter	Description
From Port / To Port	Enter the port or port list you wish to configure.

Parameter	Description
Class ID	Select the Class ID, from *0-7* to configure for the QoS parameters.
Scheduling Mechanism	*Strict* – The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weight* – Use the weighted round-robin (*WRR*) algorithm to handle packets in an even distribution in priority classes of service.

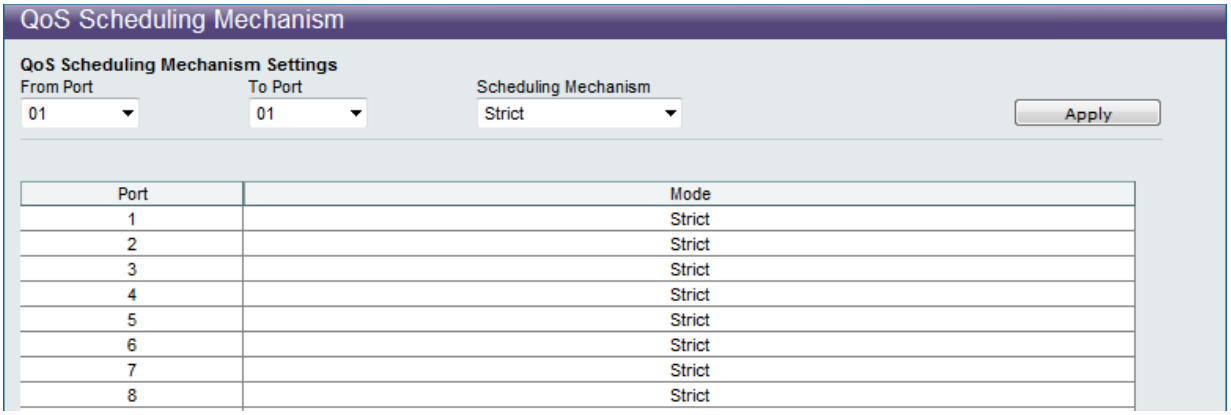
Click the **Apply** button to accept the changes made.

QoS Scheduling Mechanism

Changing the output scheduling used for the hardware queues in the Switch can customize QoS. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delays. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view this window, click **QoS > Scheduling Settings > QoS Scheduling Mechanism** as shown below:

Figure 150: QoS Scheduling Mechanism



The following parameters can be configured:

Parameter	Description
From Port / To Port	Enter the port or port list you wish to configure.
Scheduling Mechanism	*Strict* – The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weighted Round Robin* – Use the weighted round-robin algorithm to handle packets in an even distribution in priority classes of service.

Click the **Apply** button to accept the changes made.

NOTE

The settings you assign to the queues, numbers 0-7, represent the IEEE 802.1p priority tag number. Do not confuse these settings with port numbers.

7 ACL

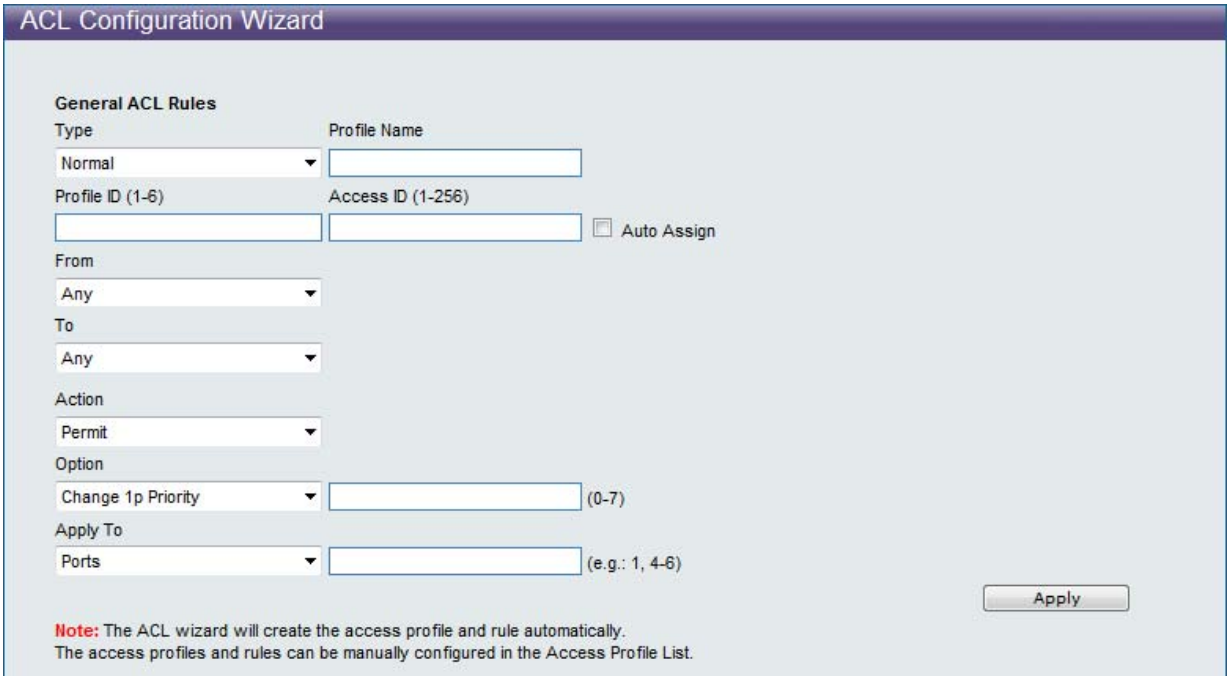
CHAPTER

ACL Configuration Wizard

The ACL Configuration Wizard will aid the user in the creation of access profiles and ACL Rules automatically by simply inputting the address or service type and the action needed. It saves administrators a lot of time.

To view this window, click **ACL > ACL Configuration Wizard** as shown below:

Figure 151: ACL Configuration Wizard window



The fields that can be configured are described below:

Parameter	Description
Type	Use the drop-down menu to select the general ACL Rule types: *Normal* – Selecting this option will create a Normal ACL Rule. *Egress* Selecting this option will create an Egress ACL Rule.

Parameter	Description
Profile Name	After selecting to configure a **Normal** type rule, the user can enter the Profile Name for the new rule here.
Profile ID	Enter the Profile ID for the new rule.
Access ID	Enter the Access ID for the new rule. Selecting the **Auto Assign** option will allow the switch to automatically assign an unused access ID to this rule.
From / To	This rule can be created to apply to four different categories: *Any* – Selecting this option will include any starting category to this rule. *MAC Address* – Selecting this option will allow the user to enter a range of MAC addresses for this rule. *IPv4 Address* – Selecting this option will allow the user to enter a range of IPv4 addresses for this rule. *IPv6* – Selecting this option will allow the user to enter a range of IPv6 addresses for this rule.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the mirror port section. Port Mirroring must be enabled and a target port must be set.
Option	After selecting the **Permit** action, the user can select one of the following options: *Change 1p Priority* – Here the user can enter the 1p priority value. *Replace DSCP* – Here the user can enter the DSCP value. *Replace ToS Precedence* – Here the user can enter the ToS Precedence value.
Apply To	Use the drop-down menu to select and enter the information that this rule will be applied to. *Ports* – Enter a port number or a port range. *VLAN Name* – Enter a VLAN name. *VLAN ID* – Enter a VLAN ID.

Click the **Apply** button to accept the changes made.

NOTE

The Switch will use one minimum mask to cover all the terms that user input, however, some extra bits may also be masked at the same time. To optimize the ACL profile and rules, please use manual configuration.

Access Profile List

Access profiles allow you to establish criteria to determine whether the Switch will forward packets based on the information contained in each packet's header.

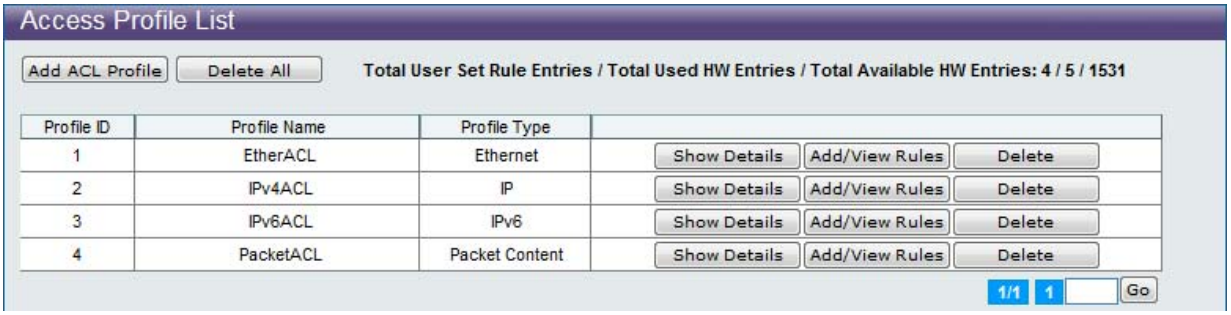
To view Access Profile List window, click **ACL > Access Profile List** as shown below:

The Switch supports four Profile Types, Ethernet ACL, IPv4 ACL, IPv6 ACL, and Packet Content ACL.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

Users can display the currently configured Access Profiles on the Switch.

Figure 152: Access Profile List window



Click the **Add ACL Profile** button to add an entry to the **Access Profile List**.

Click the **Delete All** button to remove all access profiles from this table.

Click the **Show Details** button to display the information of the specific profile ID entry.

Click the **Add/View Rules** button to view or add ACL rules within the specified profile ID.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

There are four **Add Access Profile** windows;

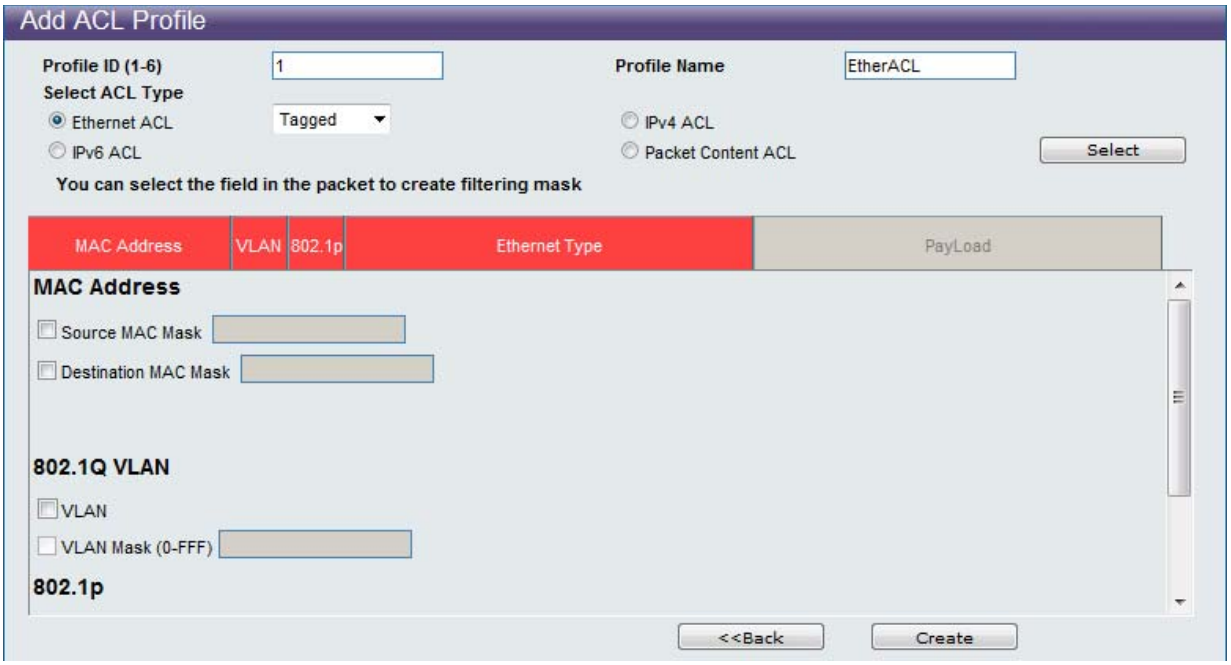
- one for Ethernet (or MAC address-based) profile configuration,
- one for IPv6 address-based profile configuration,
- one for IPv4 address-based profile configuration, and
- one for packet content profile configuration.

Add an Ethernet ACL Profile

The window shown below is the Add ACL Profile window for Ethernet. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

Figure 153: Add ACL Profile window (Ethernet ACL)



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
Source MAC Mask	Enter a MAC address mask for the source MAC address, e.g. FF-FF-FF-FF-FF-FF.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address, e.g. FF-FF-FF-FF-FF-FF.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.

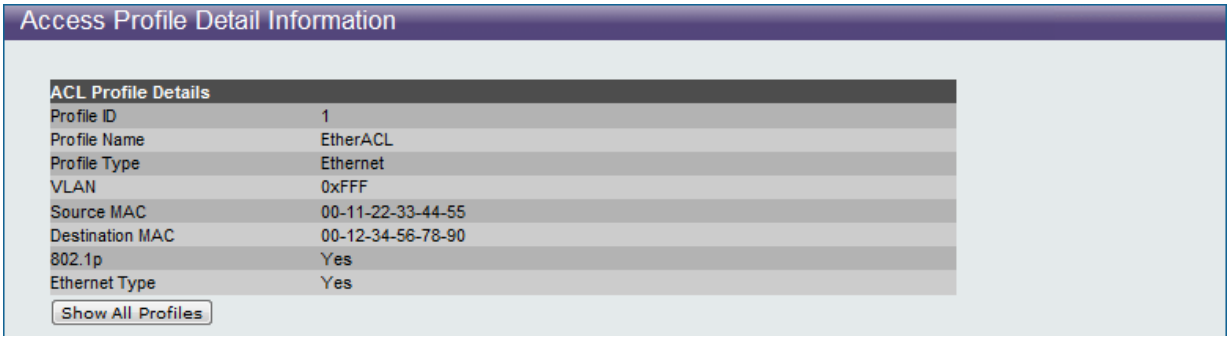
Parameter	Description
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

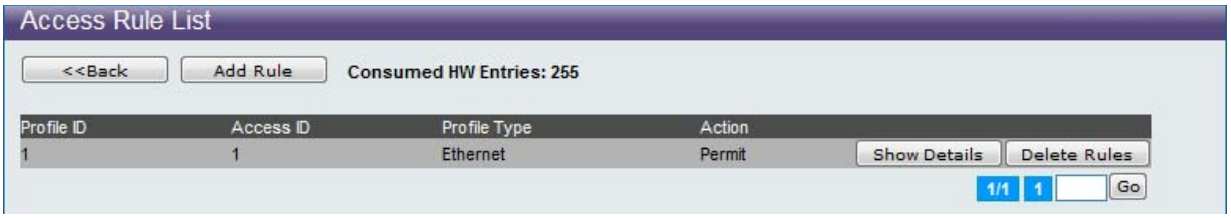
Figure 154: Access Profile Detail Information window (Ethernet ACL)



Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

Figure 155: Access Rule List window (Ethernet ACL)



Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

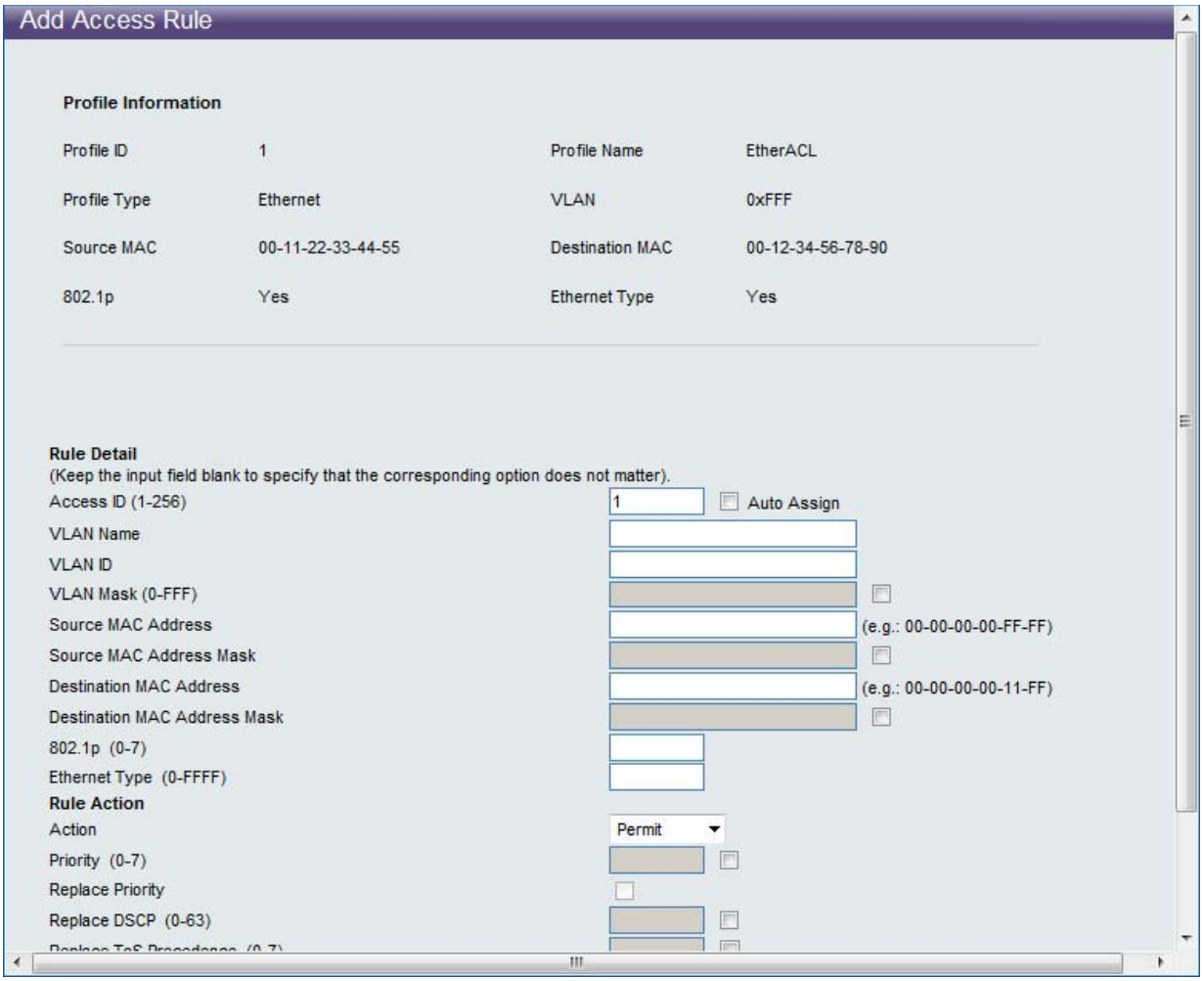
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Figure 156: Add Access Rule window (Ethernet ACL)



The fields that can be configured are described below:

Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256*.
	Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).
	Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
	Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the configure mirror port command. Port Mirroring must be enabled and a target port must be set.

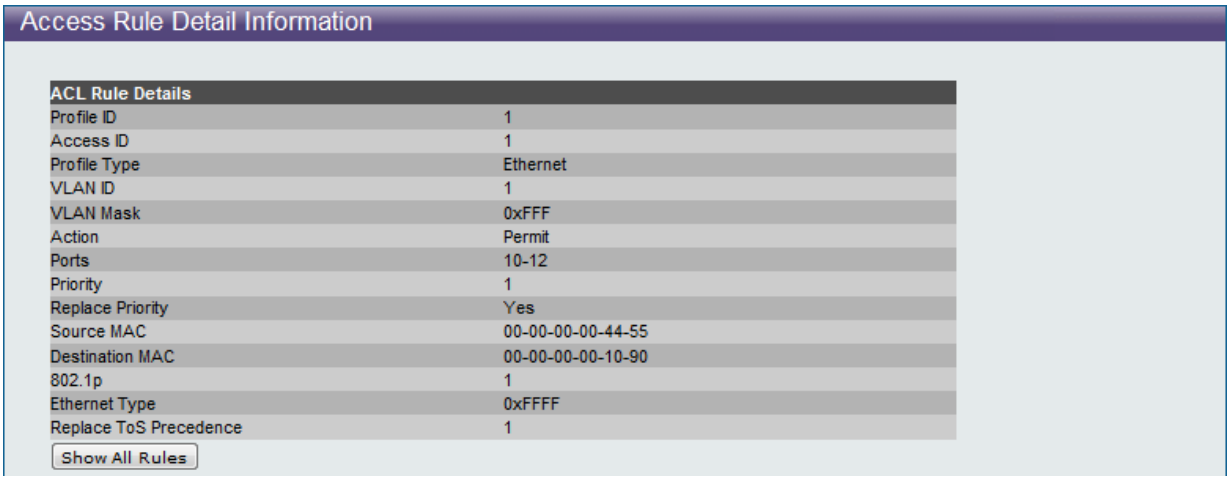
Parameter	Description
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default traffic class.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Figure 157: Access Rule Detail Information window (Ethernet ACL)



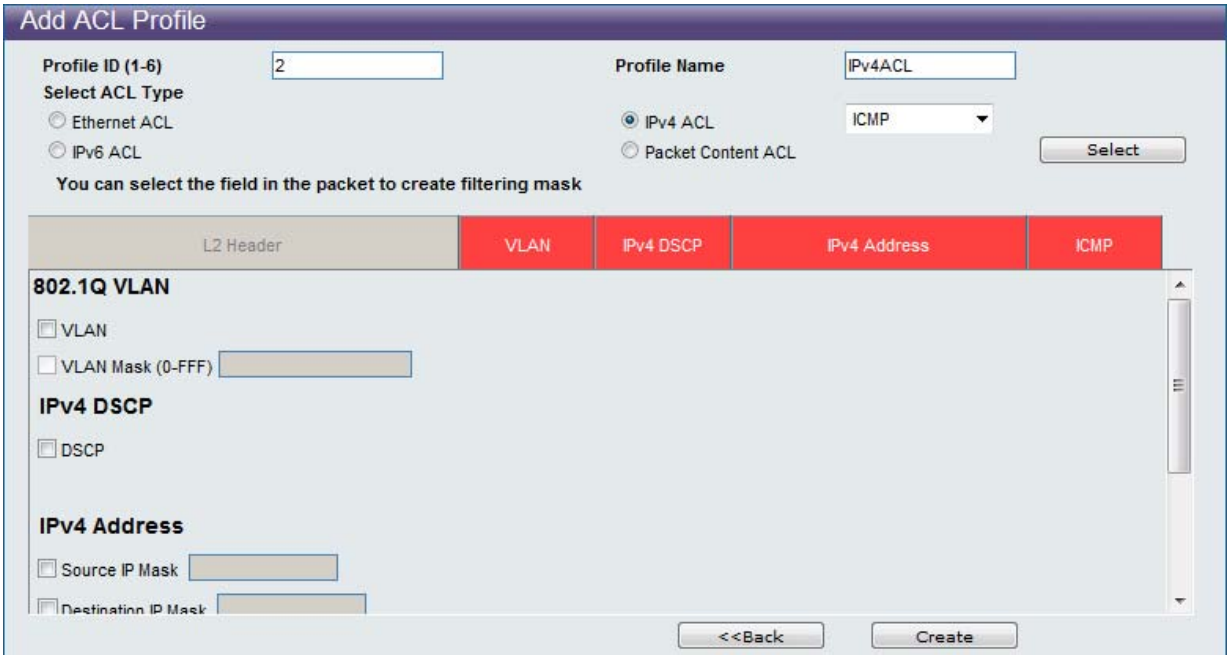
Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv4 ACL Profile

The window shown below is the Add ACL Profile window for IPv4. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

Figure 158: Add ACL Profile window (IPv4 ACL)



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile.
	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.
	Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.
	Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
	Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Source IP Mask	Enter an IP address mask for the source IP address, e.g. 255.255.255.255.

Parameter	Description
IPv4 Destination IP Mask	Enter an IP address mask for the destination IP address, e.g. 255.255.255.255.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. *flag bit* - The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff. *Protocol ID Mask* - Specify that the rule applies to the IP protocol ID traffic. *User Define* - Specify the Layer 4 part mask

Click the **Select** button to select an ACL type. Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

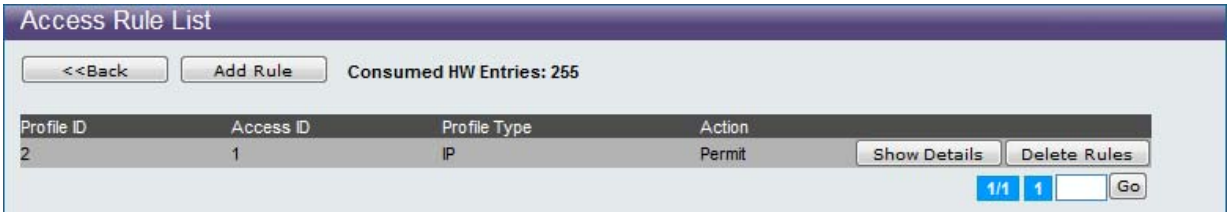
After clicking the **Show Details** button, the following page will appear:

Figure 159: Access Profile Detail Information window (IPv4 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

Figure 160: Access Rule List window (IPv4 ACL)



Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

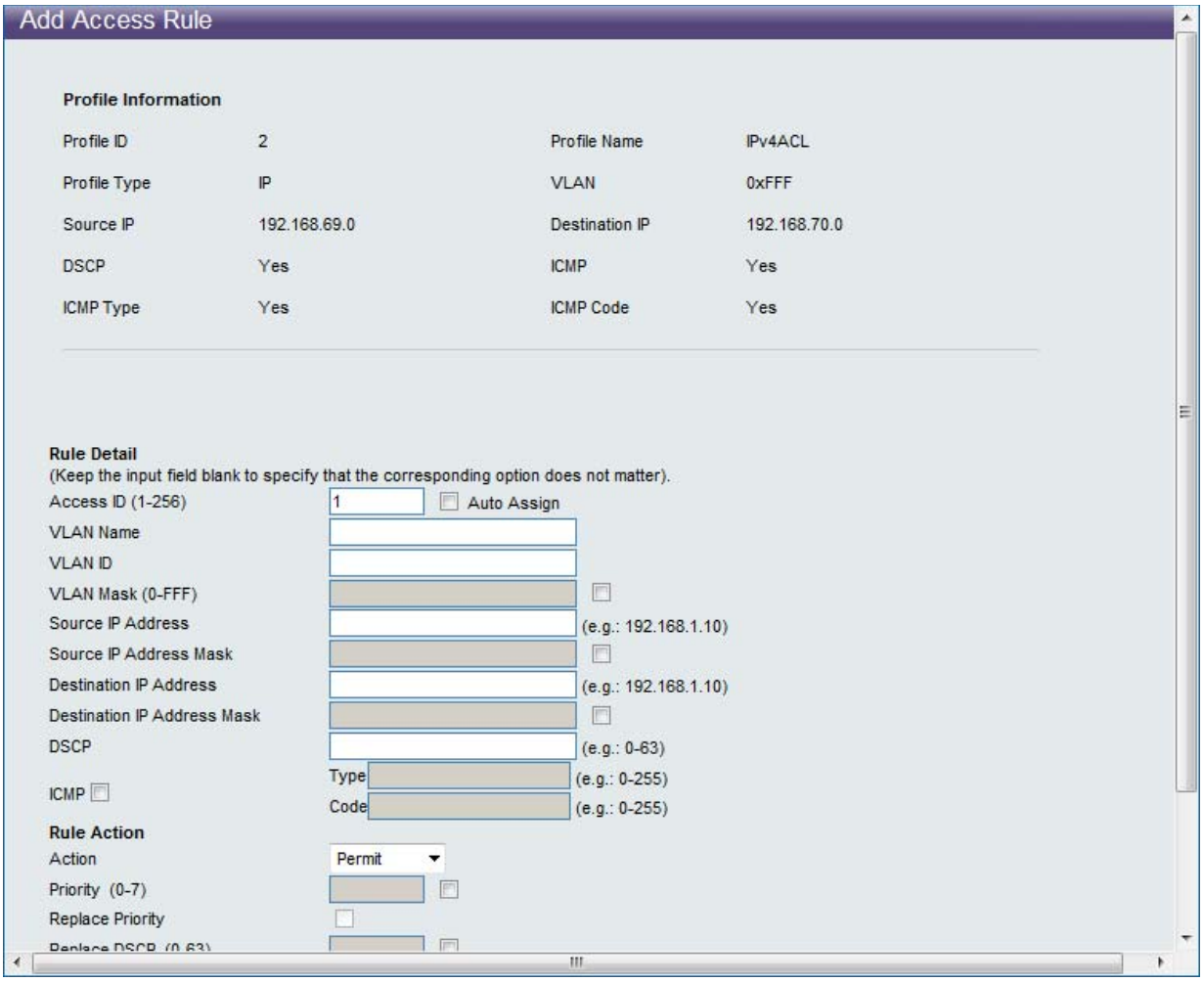
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Figure 161: Add Access Rule (IPv4 ACL)



The fields that can be configured are described below:

Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256*.
	Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).
	Select Deny to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
	Select Mirror to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.

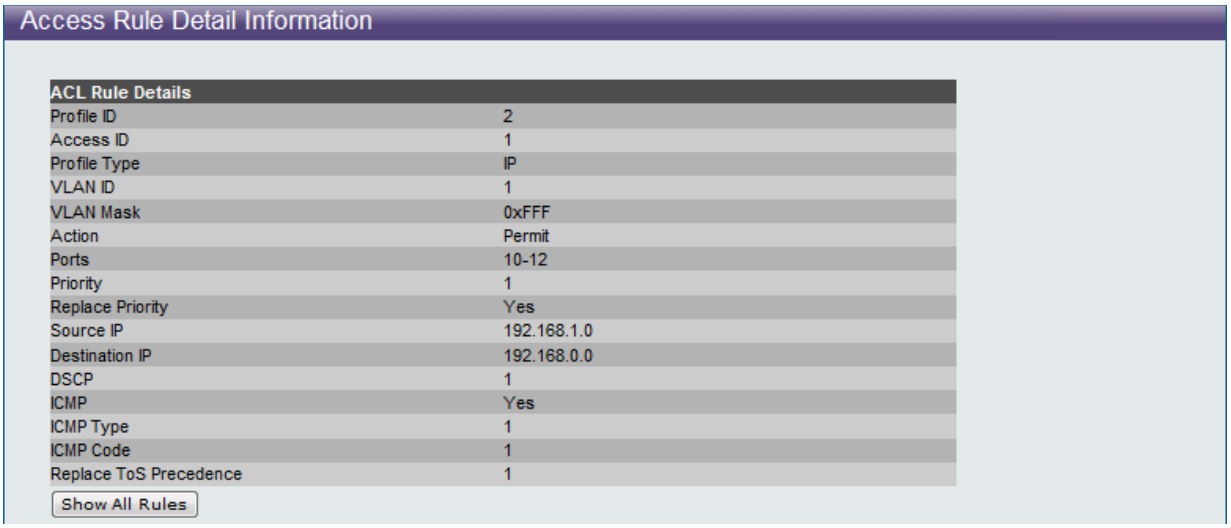
Parameter	Description
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Figure 162: Access Rule Detail Information (IPv4 ACL)



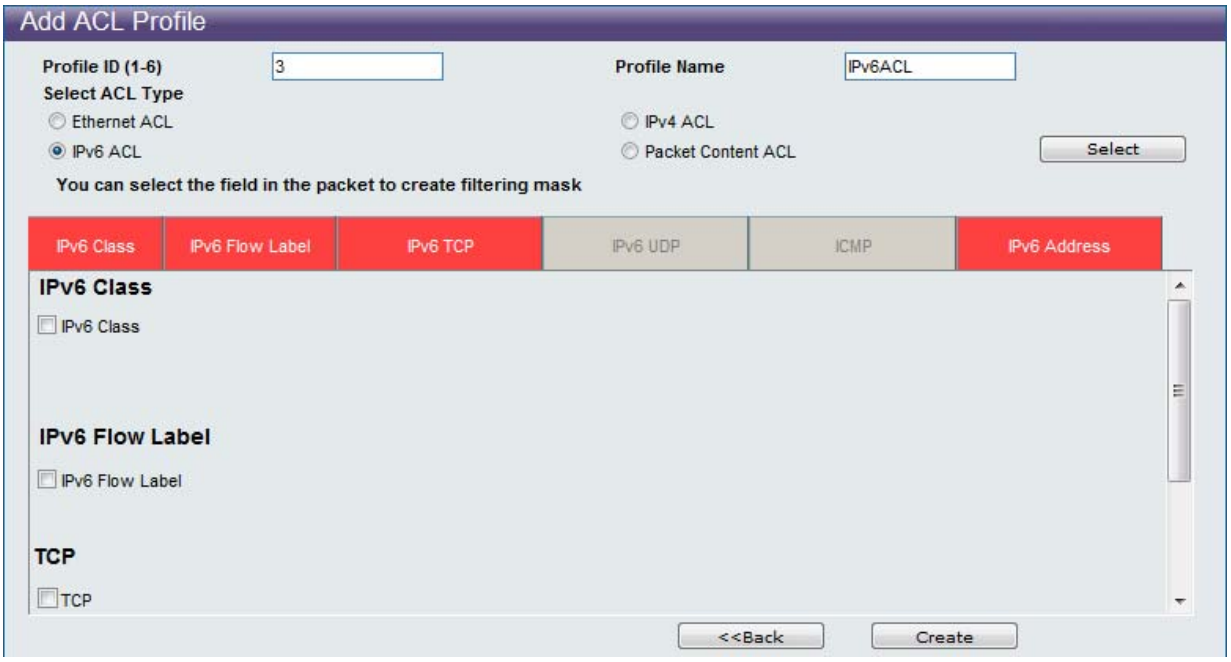
Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv6 ACL Profile

The window shown below is the Add ACL Profile window for IPv6. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

Figure 163: Add ACL Profile window (IPv6 ACL)



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile.
	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.
	Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.
	Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
	Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
IPv6 Class	Ticking this check box will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Ticking this check box will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 TCP	*Source Port Mask* – Specify that the rule applies to the range of TCP source ports.
	Destination Port Mask – Specify the range of the TCP destination port range.
IPv6 UDP	*Source Port Mask* – Specify the range of the TCP source port range.
	Destination Port Mask – Specify the range of the TCP destination port mask.

Parameter	Description
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
IPv6 Source Mask	The user may specify an IP address mask for the source IPv6 address by ticking the corresponding check box and entering the IP address mask.
IPv6 Destination Mask	The user may specify an IP address mask for the destination IPv6 address by ticking the corresponding check box and entering the IP address mask.

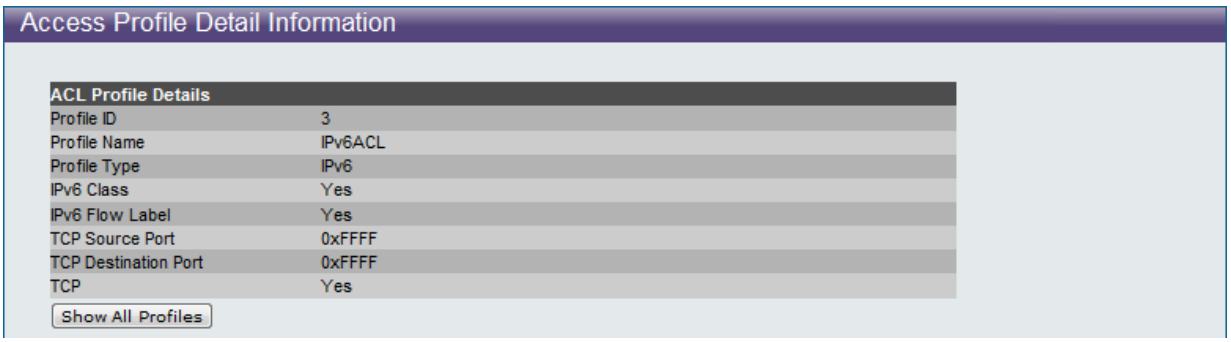
Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

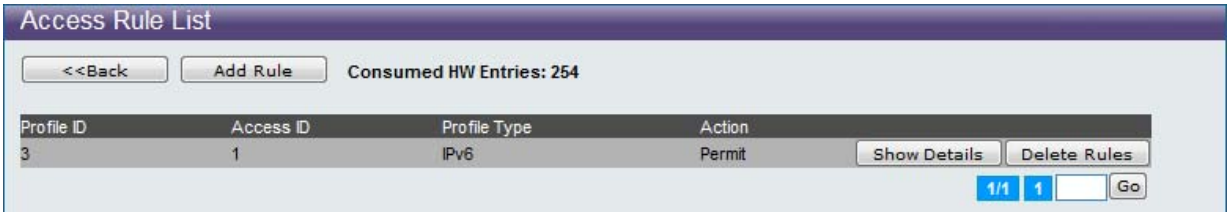
Figure 164: Access Profile Detail Information window (IPv6 ACL)



Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

Figure 165: Access Rule List window (IPv6 ACL)



Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

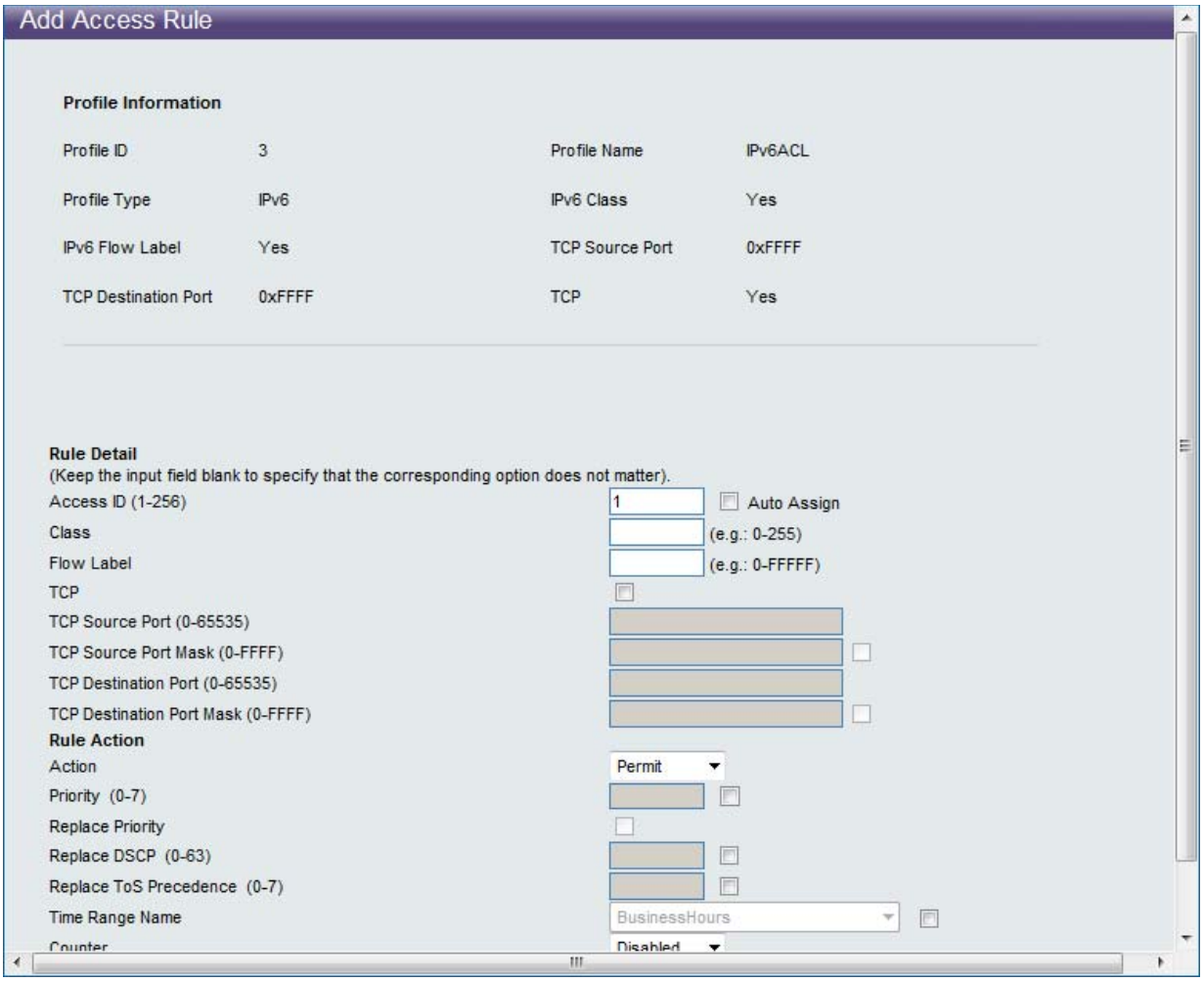
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Figure 166: Add Access Rule (IPv6 ACL)



The fields that can be configured are described below:

Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256*.
	Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).
	Select *Deny* to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
	Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.

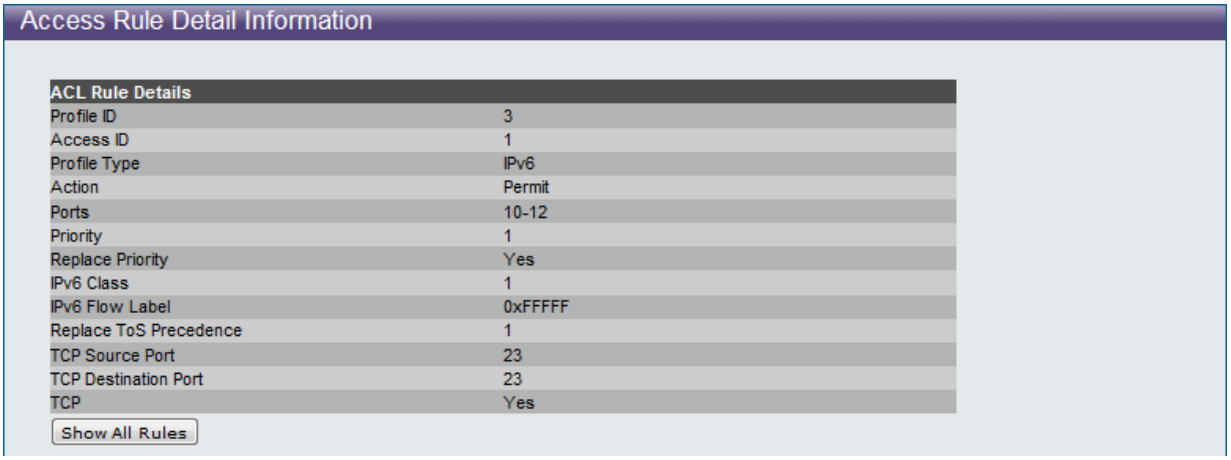
Parameter	Description
Priority (0-7)	Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv6 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Figure 167: Access Rule Detail Information (IPv6 ACL)



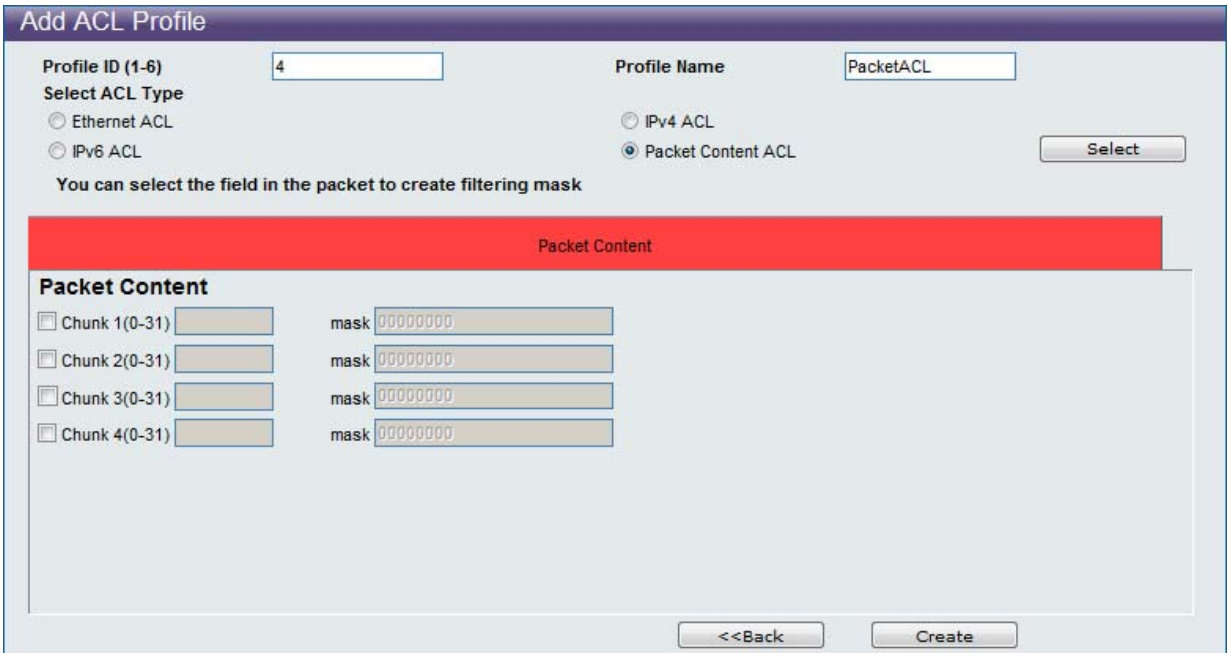
Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding a Packet Content ACL Profile

The window shown below is the Add ACL Profile window for Packet Content: To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

Figure 168: Add ACL Profile (Packet Content ACL)



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a unique identifier number for this profile set. This value can be set from *1* to *6*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile.
	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.
	Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.
	Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
	Select Packet Content to instruct the Switch to examine the packet content in each frame's header.

Parameter	Description
Packet Content	Allows users to examine up to 4 specified offset_chunks within a packet at one time and specifies the frame content offset and mask. There are 4 chunk offsets and masks that can be configured. A chunk mask presents 4 bytes. 4 offset_chunks can be selected from a possible 32 predefined offset_chunks as described below: offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4. Example: offset_chunk_1 0 0xffffffff will match packet byte offset 126,127,0,1 offset_chunk_1 0 0x0000ffff will match packet byte offset,0,1 With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the Extreme xStack® switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is why the Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

Figure 169: Access Profile Detail Information (Packet Content ACL)

Access Profile Detail Information
ACL Profile Details
Profile ID 4
Profile Name PacketACL
Profile Type Packet Content
Chunk 1 1, Value: 0x00000000
Chunk 2 2, Value: 0x00000000
Chunk 3 3, Value: 0x00000000
Chunk 4 4, Value: 0x00000000
Show All Profiles

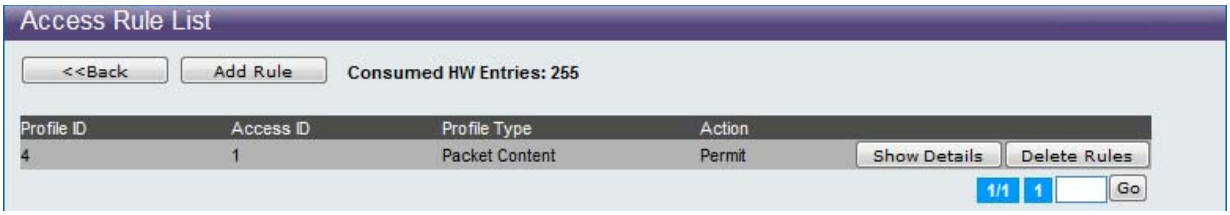
Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

NOTE

Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN (i.e. an ARP spoofing attack). For a more detailed explanation on how ARP protocol works and how to employ Extreme's unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix E at the end of this manual.

After clicking the **Add/View Rules** button, the following page will appear:

Figure 170: Access Rule List (Packet Content ACL)



Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

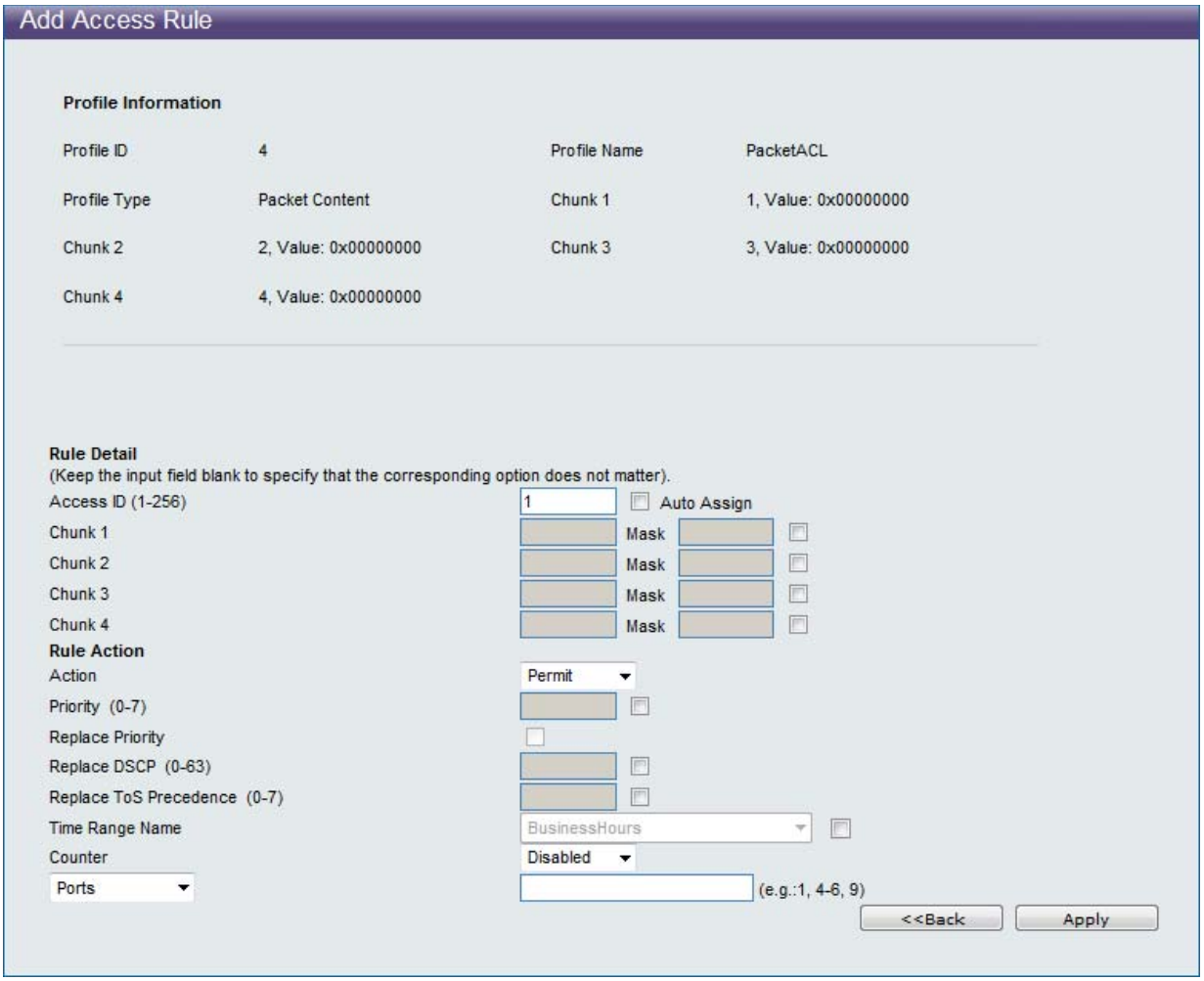
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Figure 171: Add Access Rule (Packet Content ACL)



The fields that can be configured are described below:

Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256*.
	Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).
	Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
	Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.

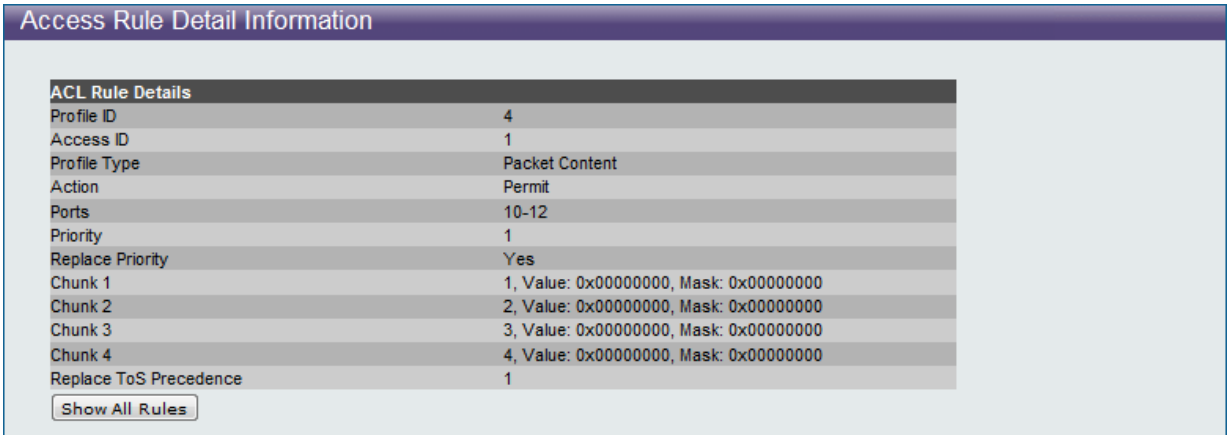
Parameter	Description
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Figure 172: Access Rule Detail Information (Packet Content ACL)


Access Rule Detail Information
ACL Rule Details
Profile ID 4
Access ID 1
Profile Type Packet Content
Action Permit
Ports 10-12
Priority 1
Replace Priority Yes
Chunk 1 1, Value: 0x00000000, Mask: 0x00000000
Chunk 2 2, Value: 0x00000000, Mask: 0x00000000
Chunk 3 3, Value: 0x00000000, Mask: 0x00000000
Chunk 4 4, Value: 0x00000000, Mask: 0x00000000
Replace ToS Precedence 1
Show All Rules

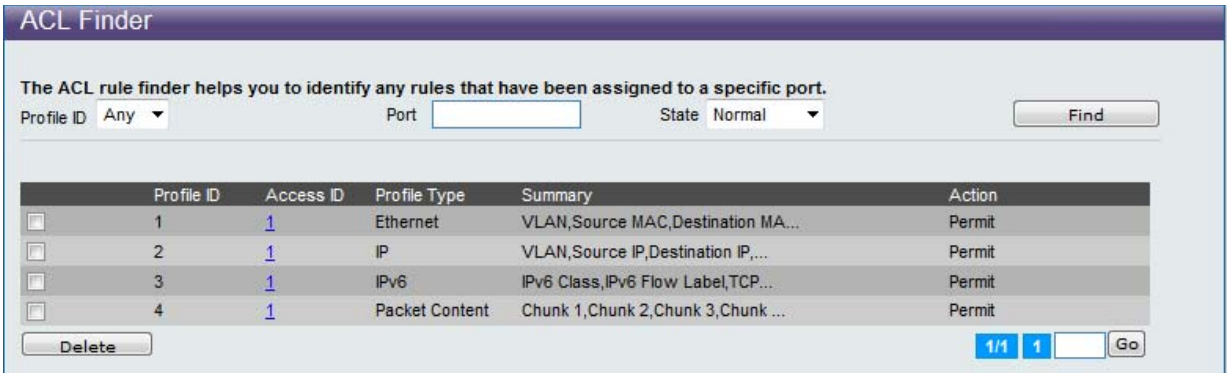
Click the **Show All Rules** button to navigate back to the Access Rule List.

ACL Finder

The ACL rule finder helps you to identify any rules that have been assigned to a specific port and edit existing rules quickly.

To view this window, click **ACL > ACL Finder** as shown below:

Figure 173: ACL Finder window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Use the drop-down menu to select the Profile ID for the ACL rule finder to identify the rule.
Port	Enter the port number for the ACL rule finder to identify the rule.
State	Use the drop-down menu to select the state.
	Normal Allow the user to find normal ACL rules.
	CPU Allow the user to find CPU ACL rules.
	Egress – Allow the user to find Egress ACL rules.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specific entry selected.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ACL Flow Meter

Before configuring the ACL Flow Meter, here is a list of acronyms and terms users will need to know.

- **trTCM** – Two Rate Three Color Marker. This, along with the srTCM, are two methods available on the switch for metering and marking packet flow. The trTCM meters and IP flow and marks it as a color based on the flow's surpassing of two rates, the CIR and the PIR.
- **CIR** – Committed Information Rate. Common to both the trTCM and the srTCM, the CIR is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. For the trTCM, the packet flow is marked green if it doesn't exceed the

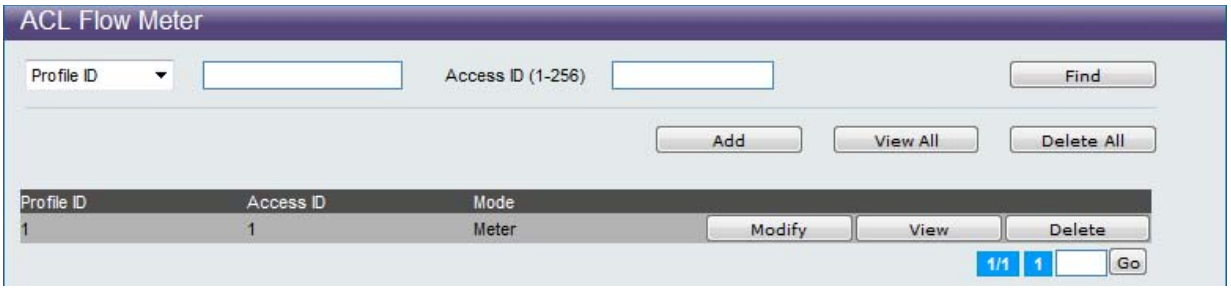
CIR and yellow if it does. The configured rate of the CIR must not exceed that of the PIR. The CIR can also be configured for unexpected packet bursts using the CBS and PBS fields.

- **CBS** – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.
- **PIR** – Peak Information Rate. This rate is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. If the packet flow exceeds the PIR, that packet flow is marked red. The PIR must be configured to be equal or more than that of the CIR.
- **PBS** – Peak Burst Size. Measured in bytes, the PBS is associated with the PIR and is used to identify packets that exceed the normal boundaries of packet size. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.
- **srTCM** – Single Rate Three Color Marker. This, along with the trTCM, are two methods available on the switch for metering and marking packet flow. The srTCM marks its IP packet flow based on the configured CBS and EBS. A packet flow that does not reach the CBS is marked green, if it exceeds the CBS but not the EBS its marked yellow, and if it exceeds the EBS its marked red.
- **CBS** – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.
- **EBS** – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS.
- **DSCP** – Differentiated Services Code Point. The part of the packet header where the color will be added. Users may change the DSCP field of incoming packets.
- The ACL Flow Meter function will allow users to color code IP packet flows based on the rate of incoming packets. Users have two types of Flow metering to choose from, trTCM and srTCM, as explained previously. When a packet flow is placed in a color code, the user can choose what to do with packets that have exceeded that color-coded rate.
- **Green** – When an IP flow is in the green mode, its configurable parameters can be set in the Conform field, where the packets can have their DSCP field changed. This is an acceptable flow rate for the ACL Flow Meter function.
- **Yellow** – When an IP flow is in the yellow mode, its configurable parameters can be set in the Exceed field. Users may choose to either Permit or Drop exceeded packets. Users may also choose to change the DSCP field of the packets.
- **Red** – When an IP flow is in the red mode, its configurable parameters can be set in the Violate field. Users may choose to either Permit or Drop exceeded packets. Users may also choose to change the DSCP field of the packets.

Users may also choose to count exceeded packets by clicking the Counter check box. If the counter is enabled, the counter setting in the access profile will be disabled. Users may only enable two counters for one flow meter at any given time.

To view this window, click **ACL** > **ACL Flow Meter**, as shown below:

Figure 174: ACL Flow Meter



The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID	Here the user can enter the Access ID for the flow meter.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

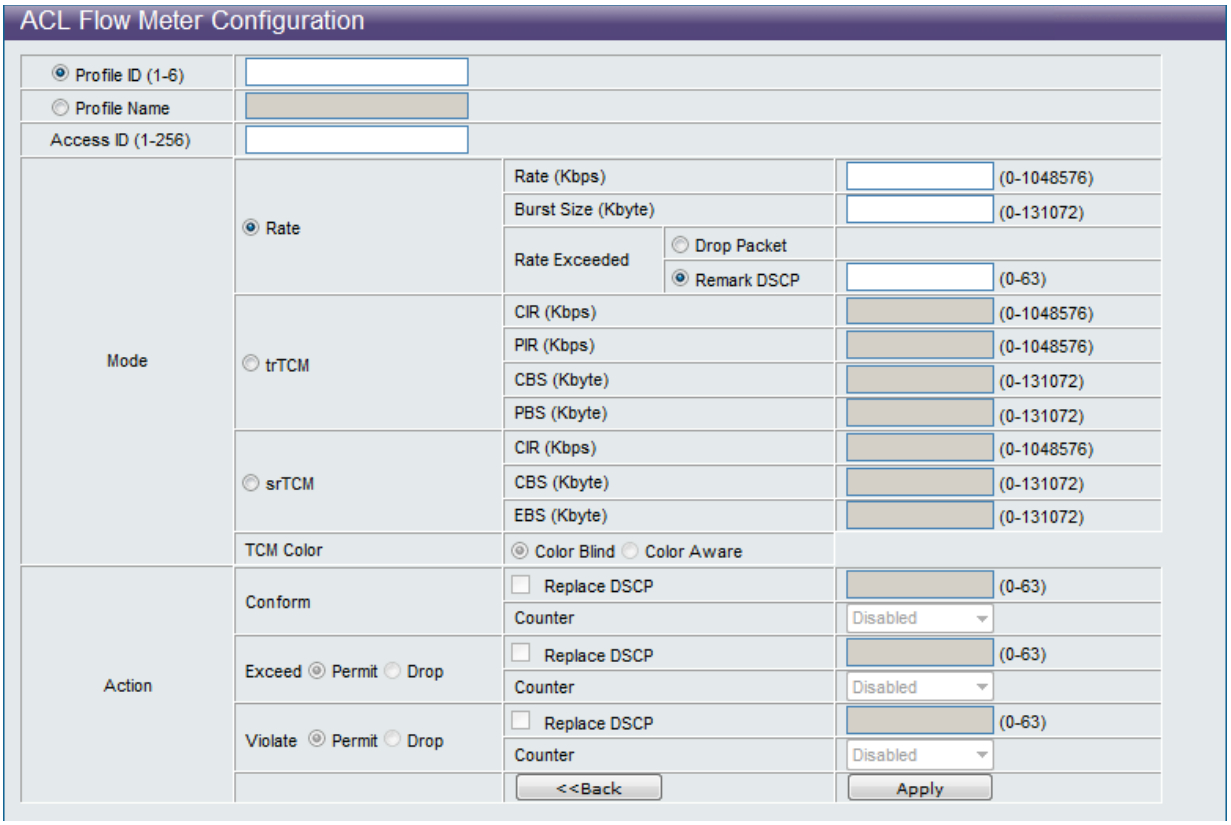
Click the **Modify** button to re-configure the specific entry.

Click the **View** button to display the information of the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Add** or **Modify** button, the following page will appear:

Figure 175: ACL Flow meter Configuration window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID	Here the user can enter the Access ID for the flow meter.

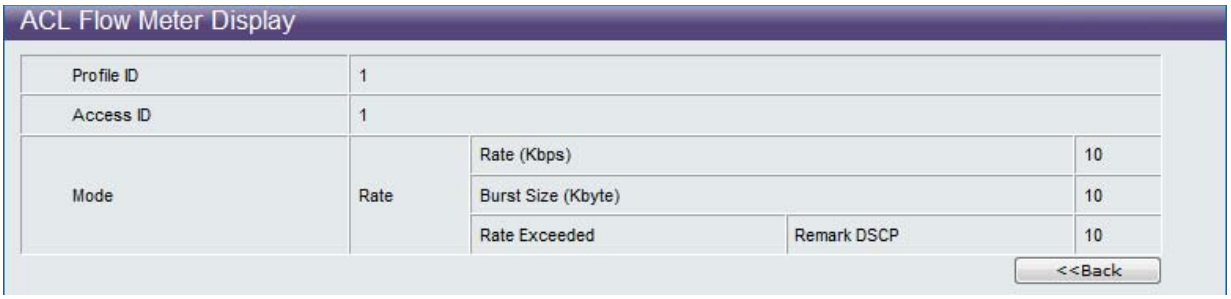
Parameter	Description
Mode	**Rate** – Specify the rate for single rate two color mode.
	Rate – Specify the committed bandwidth in Kbps for the flow.
	Burst Size – Specify the burst size for the single rate two color mode. The unit is in kilobyte.
	Rate Exceeded – Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as one of the following:
	Drop Packet – Drop the packet immediately.
	Remark DSCP – Mark the packet with a specified DSCP. The packet is set to drop for packets with a high precedence.
	trTCM – Specify the "two-rate three-color mode."
	CIR – Specify the Committed information Rate. The unit is Kbps. CIR should always be equal or less than PIR.
	PIR – Specify the Peak information Rate. The unit is Kbps. PIR should always be equal to or greater than CIR.
	CBS – Specify the Committed Burst Size. The unit is in kilobyte.
	PBS – Specify the Peak Burst Size. The unit is in kilobyte.
	srTCM – Specify the "single-rate three-color mode".
	CIR – Specify the Committed Information Rate. The unit is in kilobyte.
	CBS – Specify the Committed Burst Size. The unit is in kilobyte.
	EBS – Specify the Excess Burst Size. The unit is in kilobyte.
Action	**Conform** – This field denotes the green packet flow. Green packet flows may have their *DSCP* field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter.
	Replace DSCP – Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.
	Counter – Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.
	Exceed – This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.
	Counter – Use this parameter to enable or disable the packet counter for the specified ACL entry in the yellow flow.
	Violate – This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.
	Counter – Use this parameter to enable or disable the packet counter for the specified ACL entry in the red flow.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

After clicking the **View** button, the following page will appear:

Figure 176: ACL Flow meter Display window

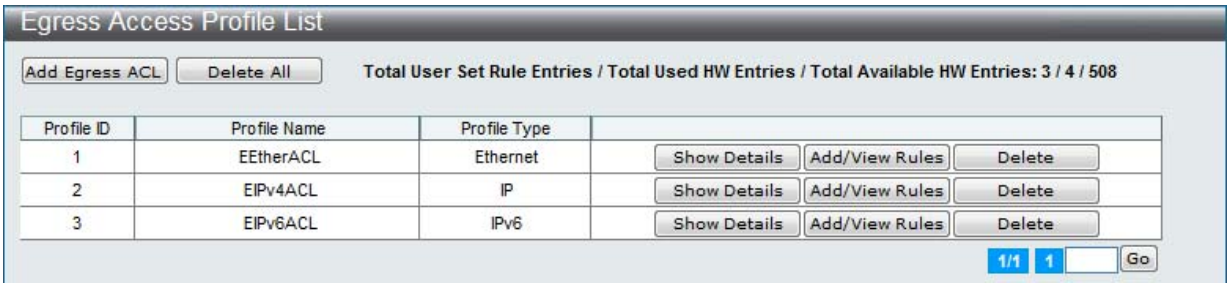


Click the **<<Back** button to return to the previous page.

Egress Access Profile List

Egress ACL performs per-flow processing of packets when they egress the Switch. The Switch supports three Profile Types, Ethernet ACL, IPv4 ACL, and IPv6 ACL.

To view this window, click **ACL > Egress Access Profile List** as shown below:



The Switch supports three Egress ACL Profile Types, Ethernet ACL, IPv4 ACL, and IPv6 ACL.

Creating an egress access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

Click the **Add Egress ACL** button to add an entry to the **Egress Access Profile List**.

Click the **Delete All** button to remove all egress access profiles from this table.

Click the **Show Details** button to display the information of the specific profile ID entry.

Click the **Add/View Rules** button to view or add ACL rules within the specified profile ID.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

There are four **Add Egress Access Profile** windows;

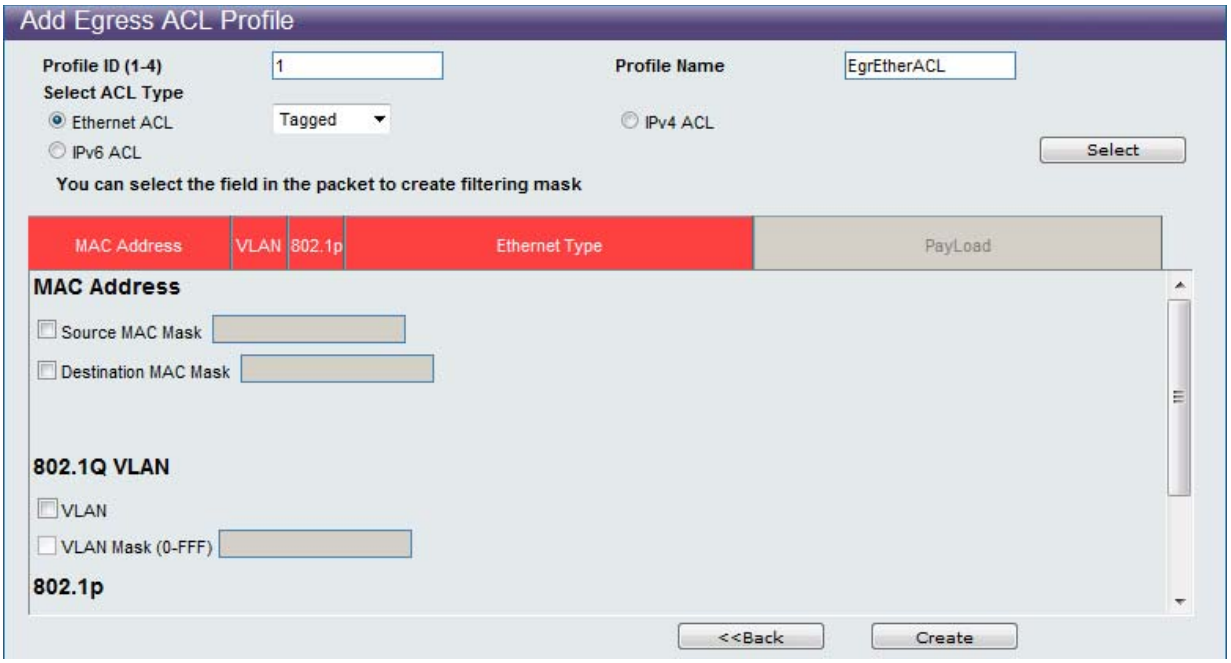
- one for Ethernet (or MAC address-based) profile configuration,
- one for IPv4 address-based profile configuration, and
- one for IPv6 address-based profile configuration.

Add an Ethernet ACL Profile

The window shown below is the Add Egress ACL Profile window for Ethernet. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

Figure 177: Add Egress ACL Profile window (Ethernet ACL)



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a unique identifier number for this profile set. This value can be set from *1* to *4*.
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.

Parameter	Description
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

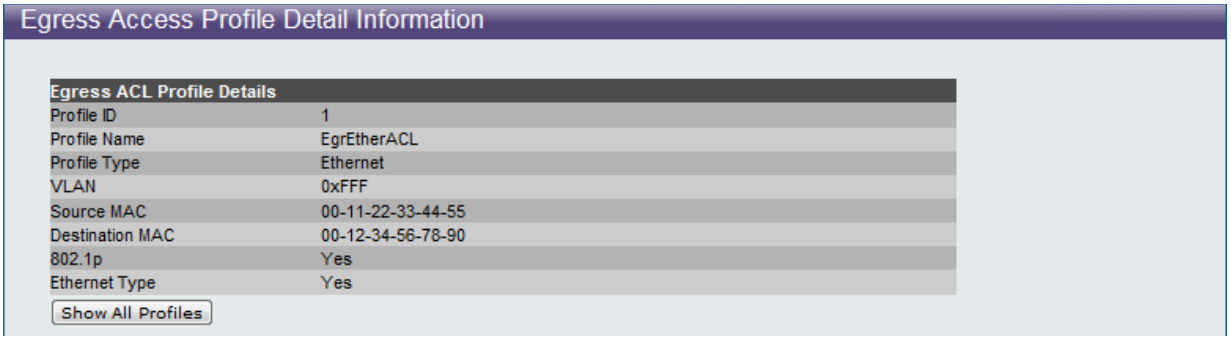
Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

Figure 178: Egress Access Profile Detail Information window (Ethernet ACL)



Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

Figure 179: Egress Access Rule List window (Ethernet ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

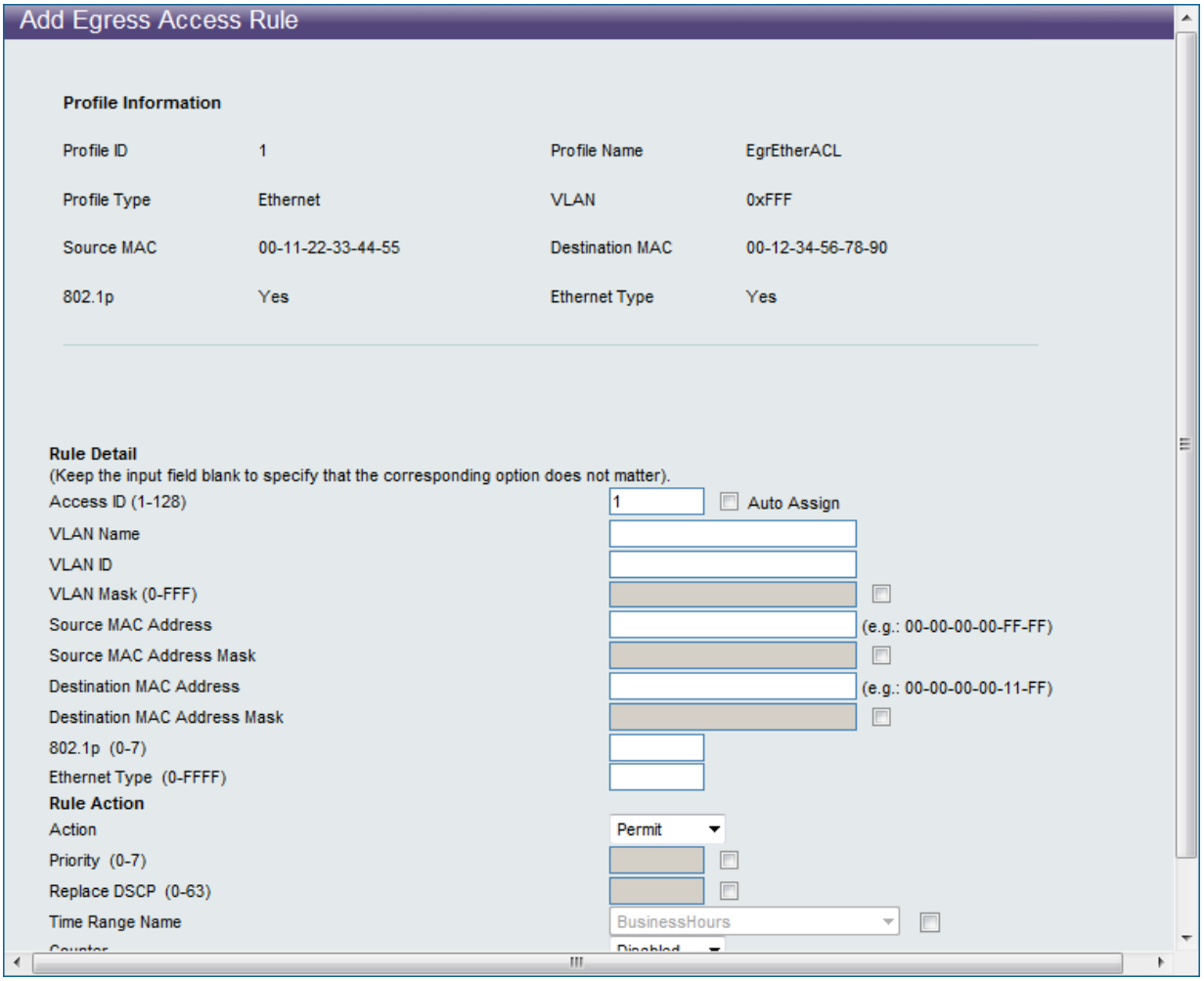
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Figure 180: Add Egress Access Rule window (Ethernet ACL)



The fields that can be configured are described below:

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. *Auto Assign* – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Ethernet Type	Specify the Ethernet type.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.

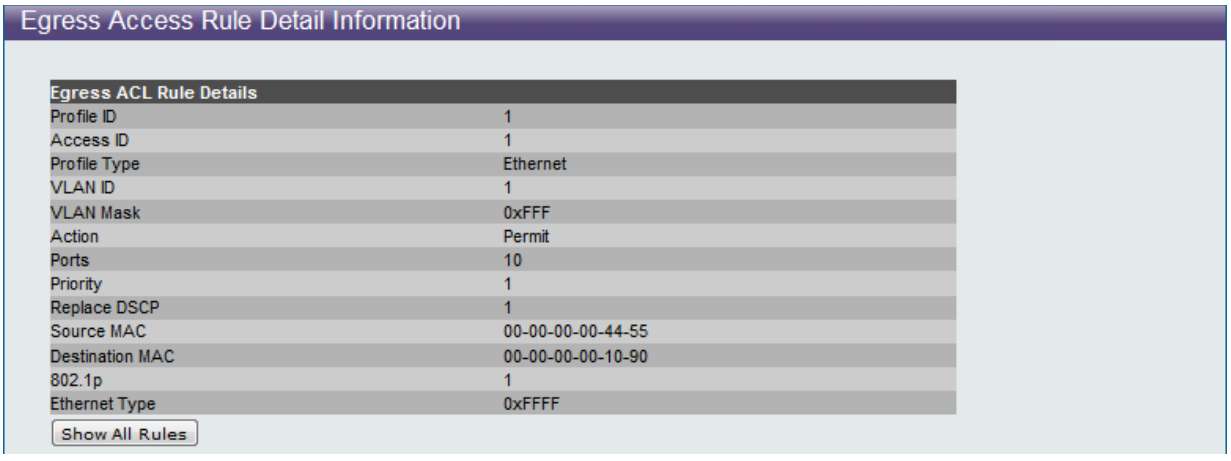
Parameter	Description
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see Chapter 6, "QoS."
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Port	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured.
Port Group ID	Specify the port group ID to apply to the access rule.
Port Group Name	Specify the port group name to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Figure 181: Egress Access Rule Detail Information window (Ethernet ACL)



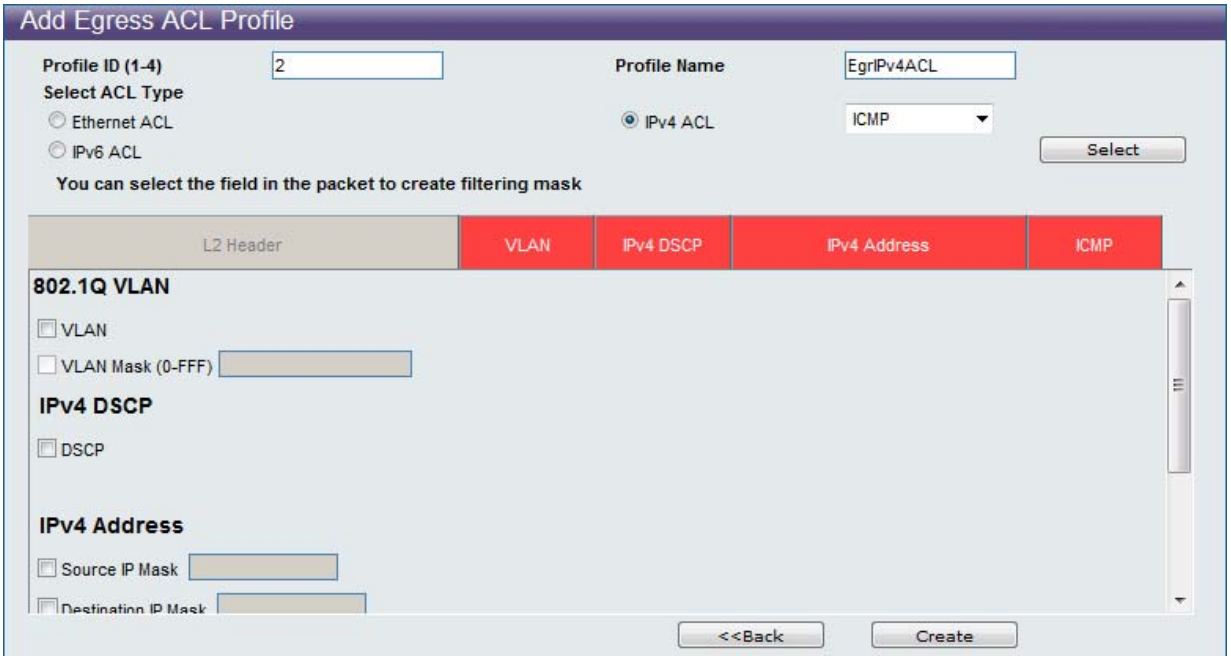
Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv4 ACL Profile

The window shown below is the Add Egress ACL Profile window for IPv4. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

Figure 182: Add Egress ACL Profile window (IPv4 ACL)



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a unique identifier number for this profile set. This value can be set from *1* to *4*.
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile.
	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.
	Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.
	Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Source IP Mask	Enter an IP address mask for the source IP address.

Parameter	Description
IPv4 Destination IP Mask	Enter an IP address mask for the destination IP address.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. *flag bit* - The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff. *Protocol ID Mask* - Specify that the rule applies to the IP protocol ID traffic. *User Define* - Specify the Layer 4 part mask

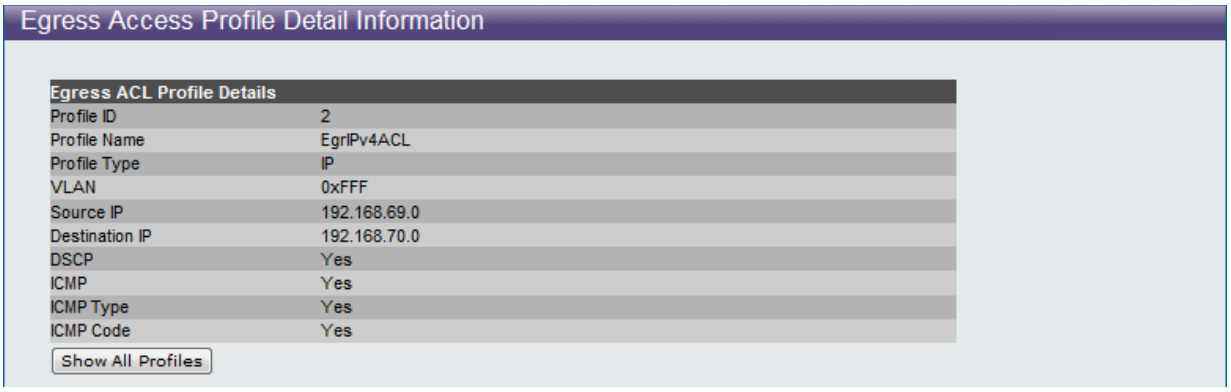
Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

Figure 183: Egress Access Profile Detail Information window (IPv4 ACL)



Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

Figure 184: Egress Access Rule List window (IPv4 ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

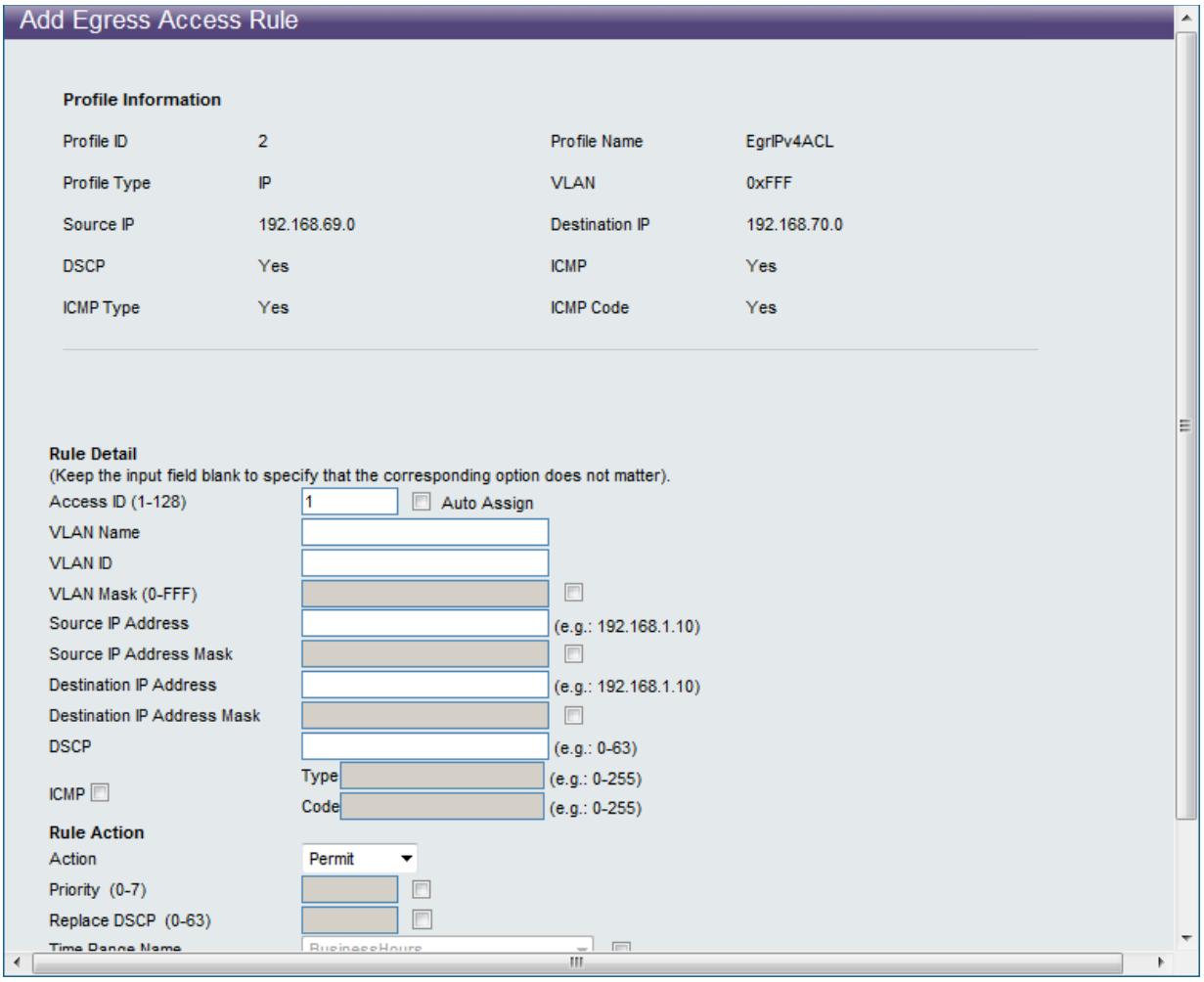
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Figure 185: Add Egress Access Rule (IPv4 ACL)



The fields that can be configured are described below:

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
DSCP	Specify the value of DSCP. The DSCP value ranges from 0 to 63.
Action	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select Deny to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.

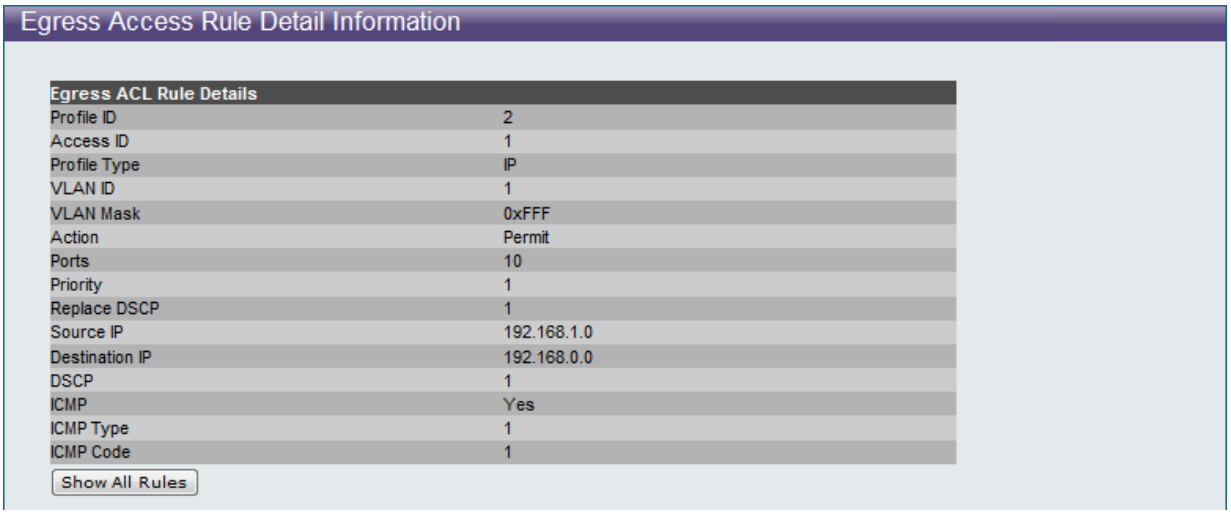
Parameter	Description
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
Port Group ID	Specify the port group ID to apply to the access rule.
Port Group Name	Specify the port group name to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Figure 186: Egress Access Rule Detail Information (IPv4 ACL)



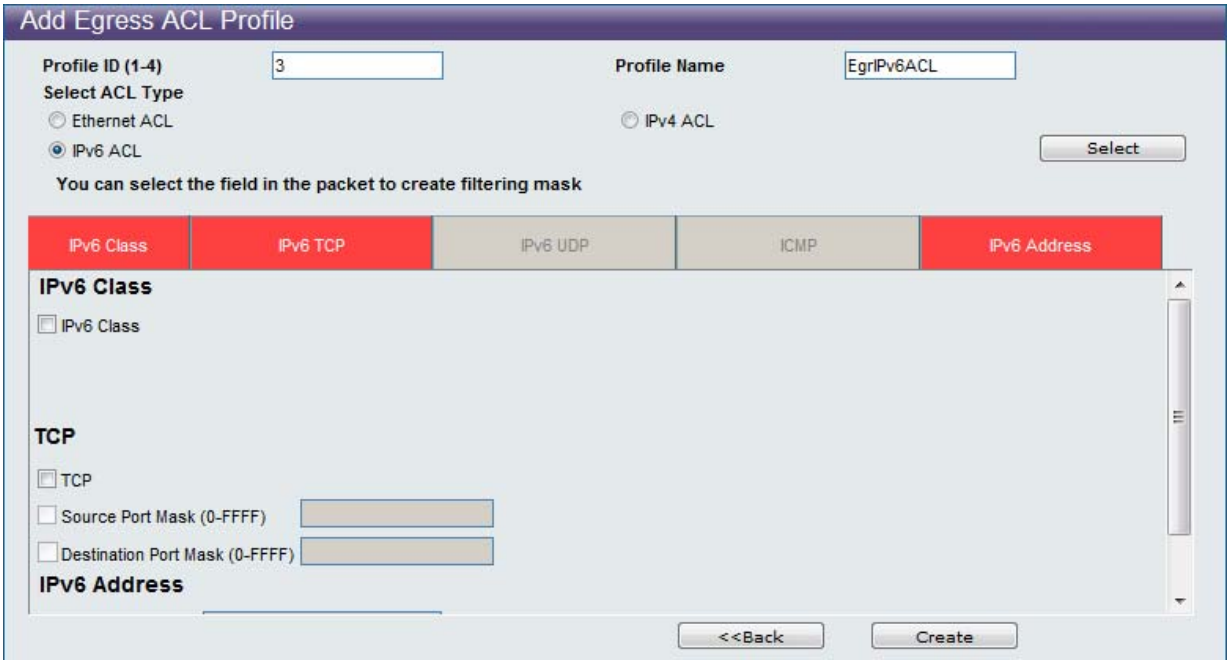
Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv6 ACL Profile

The window shown below is the Add Egress ACL Profile window for IPv6. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:

Figure 187: Add Egress ACL Profile window (IPv6 ACL)



The fields that can be configured are described below:

Parameter	Description
Profile ID	Enter a unique identifier number for this profile set. This value can be set from *1* to *4*.
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile.
	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header.
	Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header.
	Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
IPv6 Class	Ticking this check box will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 TCP	*Source Port Mask* – Specify that the rule applies to the range of TCP source ports.
	Destination Port Mask – Specify the range of the TCP destination port range.

Parameter	Description
IPv6 UDP	*Source Port Mask* – Specify the range of the UDP source port range. *Destination Port Mask* – Specify the range of the UDP destination port mask.
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
IPv6 Source Mask	The user may specify an IP address mask for the source IPv6 address by ticking the corresponding check box and entering the IP address mask, e.g. 255.255.255.255.
IPv6 Destination Mask	The user may specify an IP address mask for the destination IPv6 address by ticking the corresponding check box and entering the IP address mask, e.g. 255.255.255.255.

Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

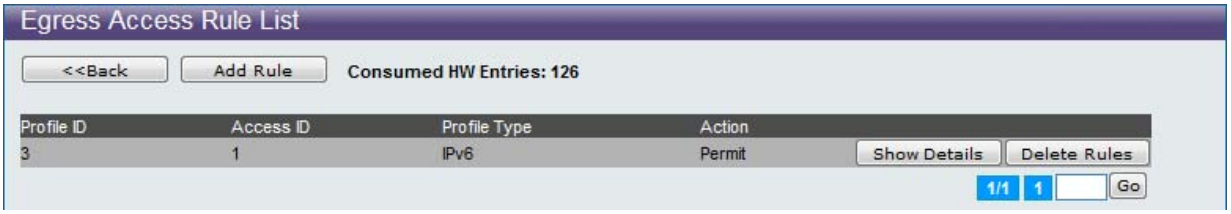
After clicking the **Show Details** button, the following page will appear:

Figure 188: Egress Access Profile Detail Information window (IPv6 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:

Figure 189: Egress Access Rule List window (IPv6 ACL)



Click the **Add Rule** button to create a new ACL rule in this profile.

Click the **<<Back** button to return to the previous page.

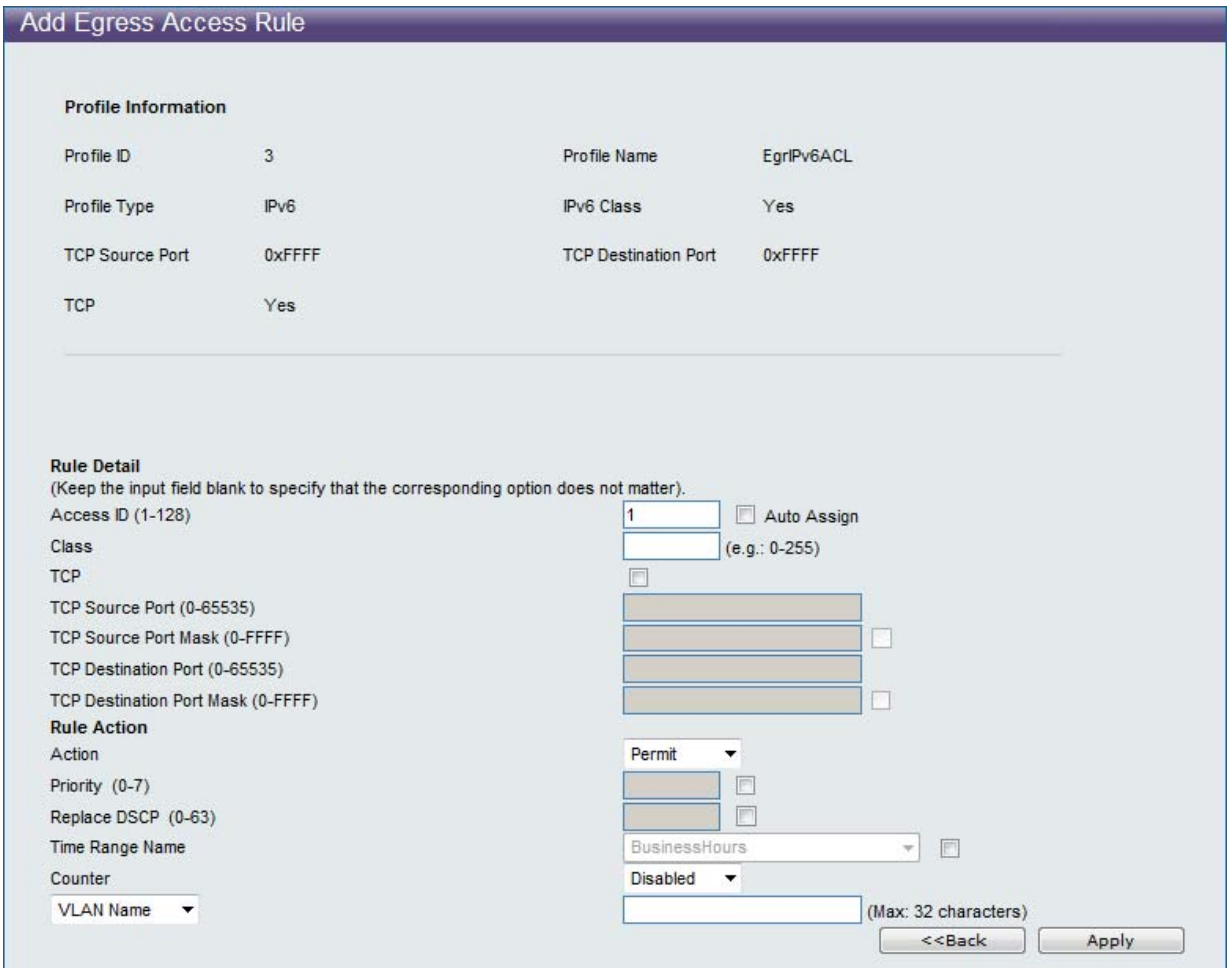
Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:

Figure 190: Add Egress Access Rule (IPv6 ACL)



The fields that can be configured are described below:

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Class	Specify the value of IPv6 class.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.

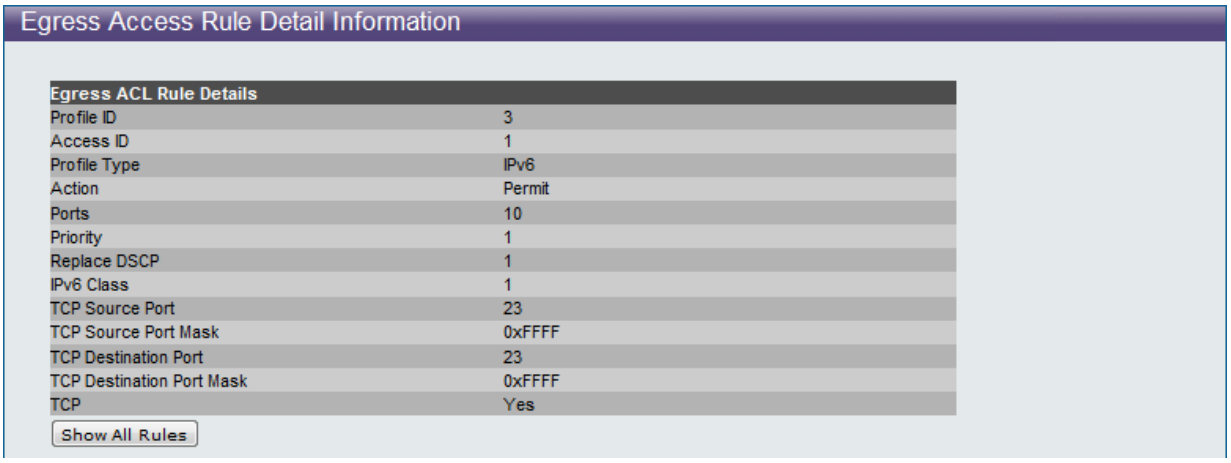
Parameter	Description
Priority (0-7)	Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv6 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
Port Group ID	Specify the port group ID to apply to the access rule.
Port Group Name	Specify the port group name to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:

Figure 191: Egress Access Rule Detail Information (IPv6 ACL)



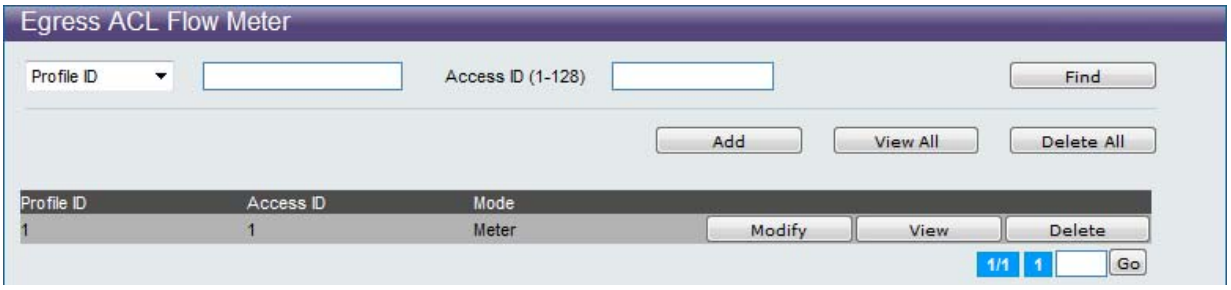
Click the **Show All Rules** button to navigate back to the Access Rule List.

Egress ACL Flow Meter

This window is used to configure the packet flow-based metering based on an egress access profile and rule.

To view this window, click **ACL > Egress ACL Flow Meter** as shown below:

Figure 192: Egress ACL Flow Meter window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID	Here the user can enter the Access ID for the flow meter.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

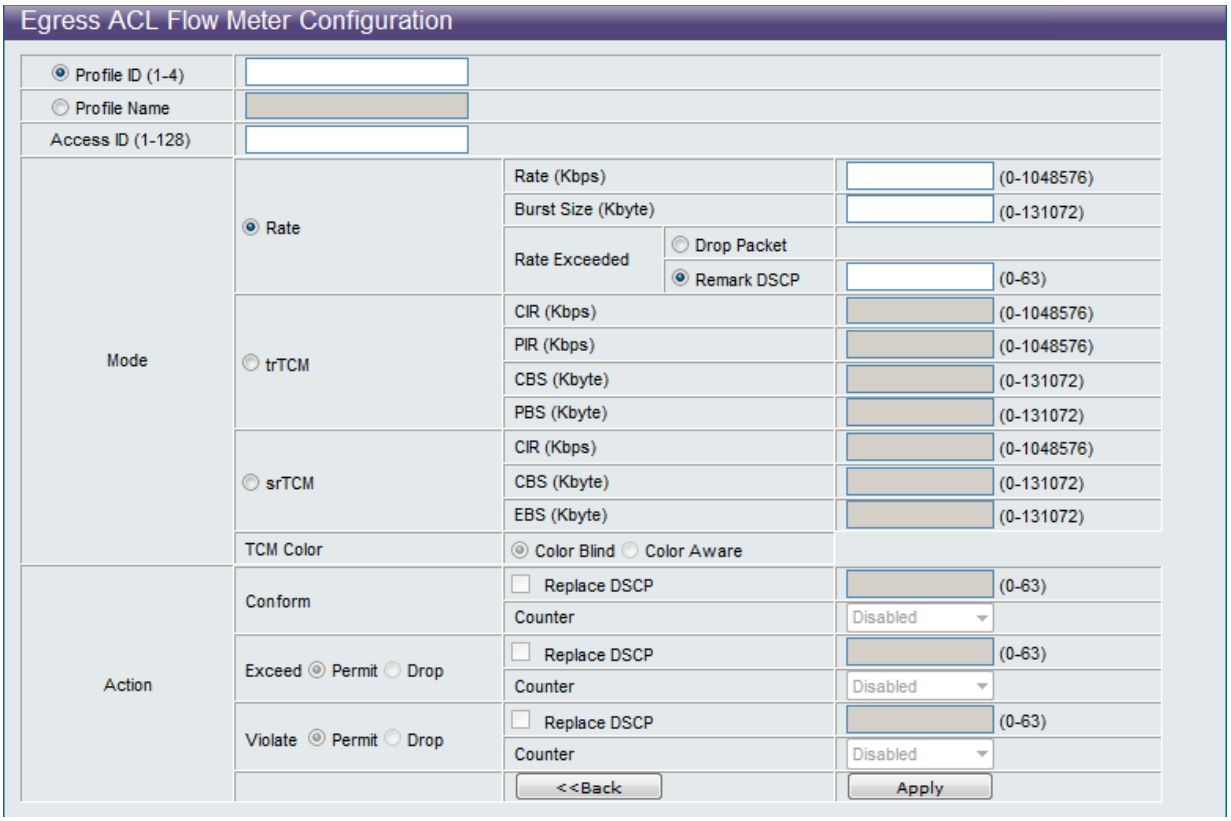
Click the **Modify** button to re-configure the specific entry.

Click the **View** button to display the information of the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Add** or **Modify** button, the following page will appear:

Figure 193: Egress ACL Flow Meter Configuration window



The fields that can be configured are described below:

Parameter	Description
Profile ID	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID	Here the user can enter the Access ID for the flow meter.

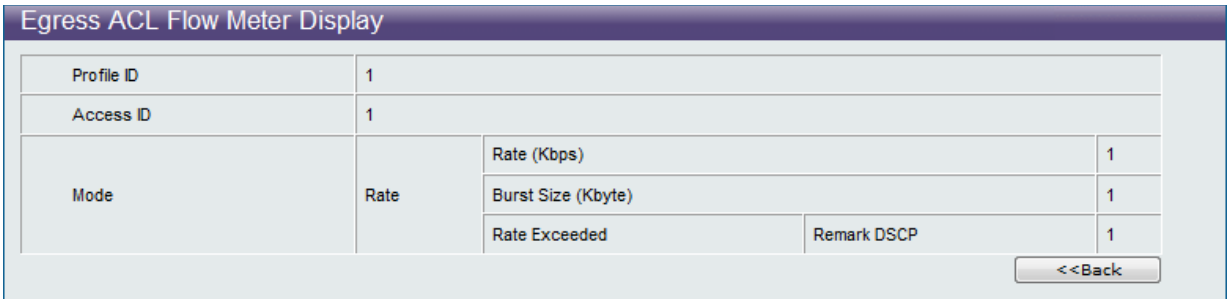
Parameter	Description
Mode	**Rate** – Specify the rate for single rate two color mode.
	Rate – Specify the committed bandwidth in Kbps for the flow.
	Burst Size – Specify the burst size for the single rate two color mode. The unit is in kilobyte.
	Rate Exceeded – Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as one of the following:
	Drop Packet – Drop the packet immediately.
	Remark DSCP – Mark the packet with a specified DSCP. The packet is set to drop for packets with a high precedence.
	trTCM – Specify the "two-rate three-color mode."
	CIR – Specify the Committed information Rate. The unit is Kbps. CIR should always be equal or less than PIR.
	PIR – Specify the Peak information Rate. The unit is Kbps. PIR should always be equal to or greater than CIR.
	CBS – Specify the Committed Burst Size. The unit is in kilobyte.
	PBS – Specify the Peak Burst Size. The unit is in kilobyte.
	srTCM – Specify the "single-rate three-color mode".
	CIR – Specify the Committed Information Rate. The unit is in kilobyte.
	CBS – Specify the Committed Burst Size. The unit is in kilobyte.
	EBS – Specify the Excess Burst Size. The unit is in kilobyte.
Action	**Conform** – This field denotes the green packet flow. Green packet flows may have their *DSCP* field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter.
	Replace DSCP – Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace.
	Counter – Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow.
	Exceed – This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.
	Counter – Use this parameter to enable or disable the packet counter for the specified ACL entry in the yellow flow.
	Violate – This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field.
	Counter – Use this parameter to enable or disable the packet counter for the specified ACL entry in the red flow.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

After clicking the **View** button, the following page will appear:

Figure 194: Egress ACL Flow meter Display window



Click the **<<Back** button to return to the previous page.

8 Security

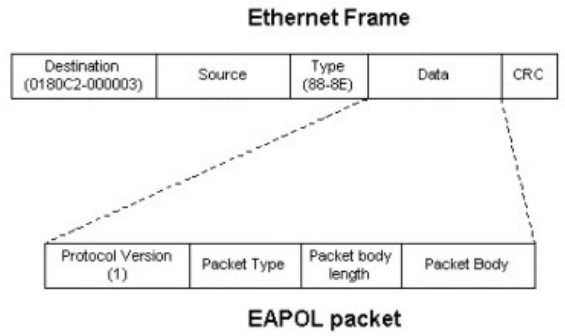
CHAPTER

802.1X

802.1X (Port-Based and Host-Based Access Control)

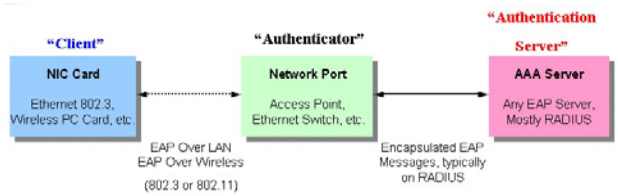
The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:

Figure 195: The EAPOL Packet



Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X Access Control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

Figure 196: The three roles of 802.1X

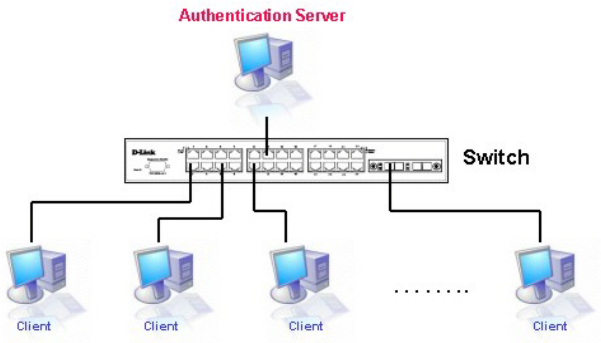


The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

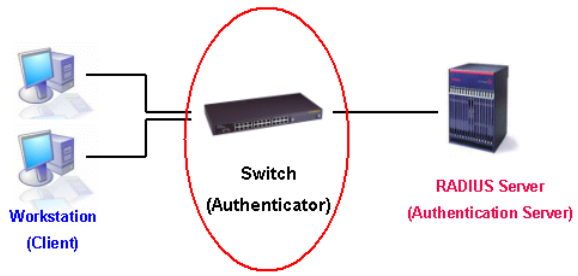
Figure 197: The Authentication Server



Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

Figure 198: The Authenticator



Three steps must be implemented on the Switch to properly configure the Authenticator.

1 The 802.1X State must be *Enabled*. (**Security / 802.1X /802.1X Settings**)

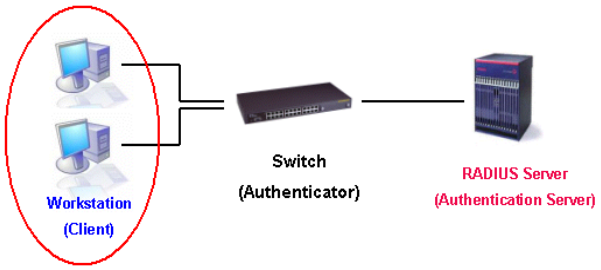
2 The 802.1X settings must be implemented by port (**Security / 802.1X / 802.1X Settings**)

3 A RADIUS server must be configured on the Switch. (**Security / 802.1X / Authentic RADIUS Server**)

Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows XP and Windows Vista, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

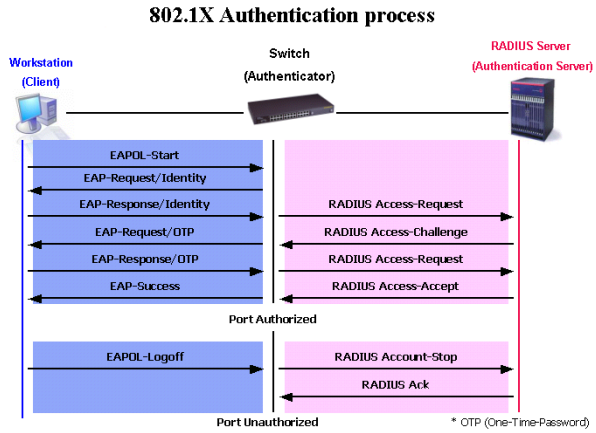
Figure 199: The Client



Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

Figure 200: The 802.1X Authentication Process



The Extreme implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

1 Port-Based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.

2 Host-Based Access Control – Using this method, the Switch will automatically learn up to a maximum of 448 MAC addresses by port and set them in a list. Each MAC address must be

authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

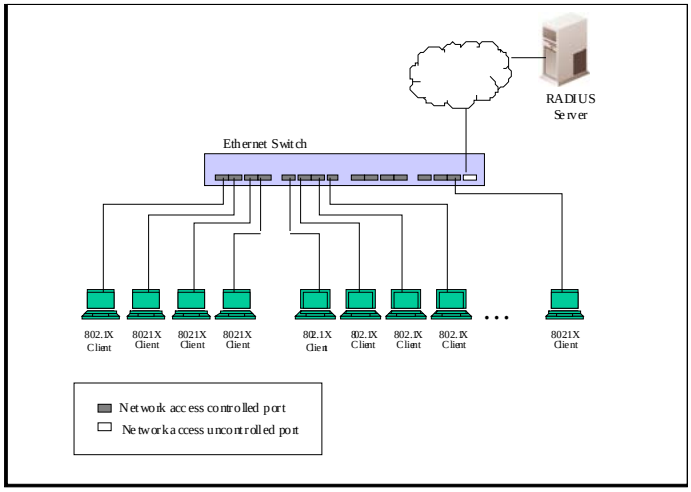
Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

Port-Based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

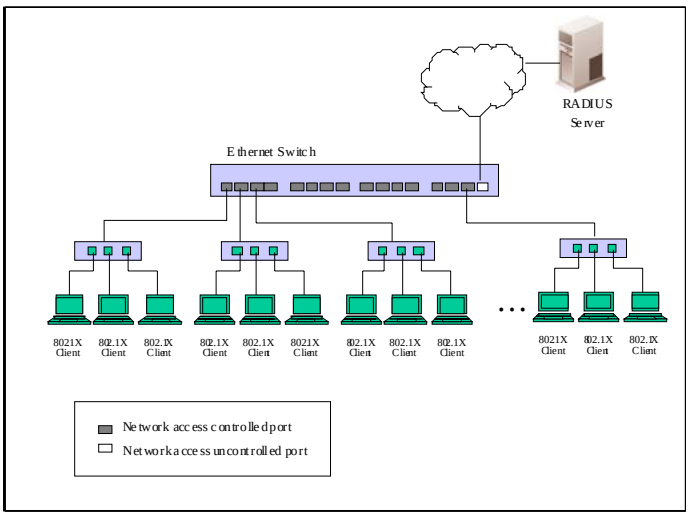
Figure 201: Example of Typical Port-based Configuration



Host-Based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

Figure 202: Example of Typical Host-based Configuration



802.1X Global Settings

Users can configure the 802.1X global parameter.

To view this window, click **Security > 802.1X > 802.1X Global Settings** as shown below:

Figure 203: 802.1X Global Settings window

The fields that can be configured are described below:

Parameter	Description
Authentication Mode	Choose the 802.1X authenticator mode, *Disabled*, *Port-based*, or *MAC-based*.
Authentication Protocol	Choose the authenticator protocol, *Local* or *RADIUS EAP*.
Forward EAPOL PDU	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Max Users	Specifies the maximum number of users. The limit on the maximum users is *448* users. This the **No Limit** check box to have unlimited users.
RADIUS Authorization	This option is used to enable or disable acceptation of authorized configuration. When the authorization is enabled for 802.1X's RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled.

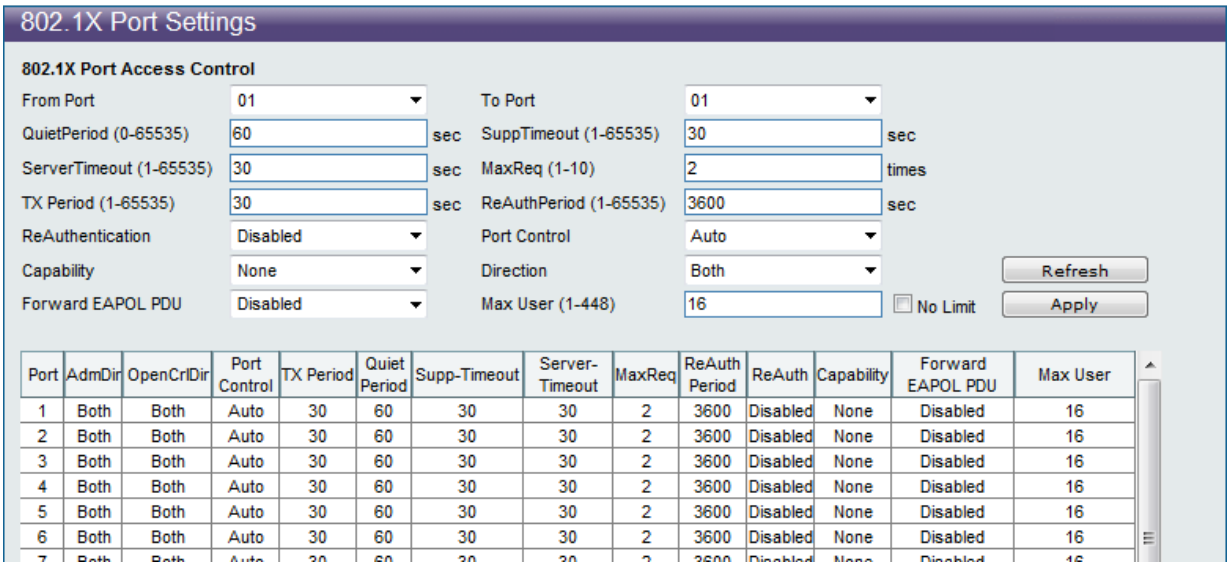
Click the **Apply** button to accept the changes made.

802.1X Port Settings

Users can configure the 802.1X authenticator port settings.

To view this window, click **Security > 802.1X > 802.1X Port Settings** as shown below:

Figure 204: 802.1X Port Settings



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports you wish to configure.
QuietPeriod	This allows the user to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds. It is defined in SuppTimeout, IEEE-802.1X-2001, page 47. The initialization value is used for the awhile timer when timing out the Supplicant. Its default value is 30 seconds; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly. It can be set by management to any value in the range from 1 to 65535 seconds.
ServerTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is *2*. It is defined in MaxReq, IEEE-802.1X-2001 page 47. The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session. Its default value is 2; it can be set by management to any value in the range from 1 to 10.

Parameter	Description
TxPeriod	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.
ReAuthPeriod	A constant that defines a nonzero number of seconds between periodic re-authentication of the client. The default setting is *3600* seconds.
ReAuthentication	Determines whether regular re-authentication will take place on this port. The default setting is *Disabled*.
Port Control	This allows the user to control the port authorization state. Select *ForceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *ForceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. If *Auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is *Auto*.
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select *Authenticator* to apply the settings to the port. When the setting is activated, a user must pass the authentication process to gain access to the network. Select *None* disable 802.1X functions on the port.
Direction	Sets the administrative-controlled direction to *Both* or *In.* If *Both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. If *In* is selected, the control is only exerted over incoming traffic through the port the user selected in the first field.
Forward EAPOL PDU	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Max Users	Specifies the maximum number of users. The maximum user limit is 448 users. The default is 16.

Click the **Refresh** button to refresh the display table so that new entries will appear.

Click the **Apply** button to accept the changes made.

802.1X User Settings

Users can set different 802.1X users in switch's local database.

To view this window, click **Security > 802.1X > 802.1X User Settings** as shown below:

Figure 205: 802.1X User Settings window

The fields that can be configured are described below:

Parameter	Description
802.1X User	The user can enter an 802.1X user's username in here.
Password	The user can enter an 802.1X user's password in here.
Confirm Password	The user can re-enter an 802.1X user's password in here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

NOTE

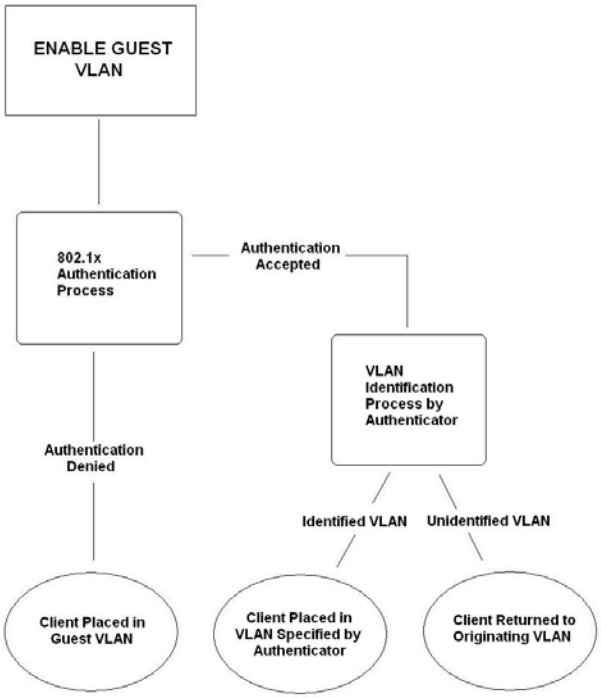
The **802.1X User** and **Password** values should be less than 16 characters.

Guest VLAN Settings

On 802.1X security-enabled networks, there is a need for non- 802.1X supported devices to gain limited access to the network, due to lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or older operating systems, or the need for guests to gain access to the network without full authorization or local authentication on the Switch. To supplement these circumstances, this switch now implements 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement 802.1X Guest VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN.

Figure 206: Guest VLAN Authentication Process



If authenticated and the authenticator possess the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

Limitations Using the Guest VLAN

1 Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.

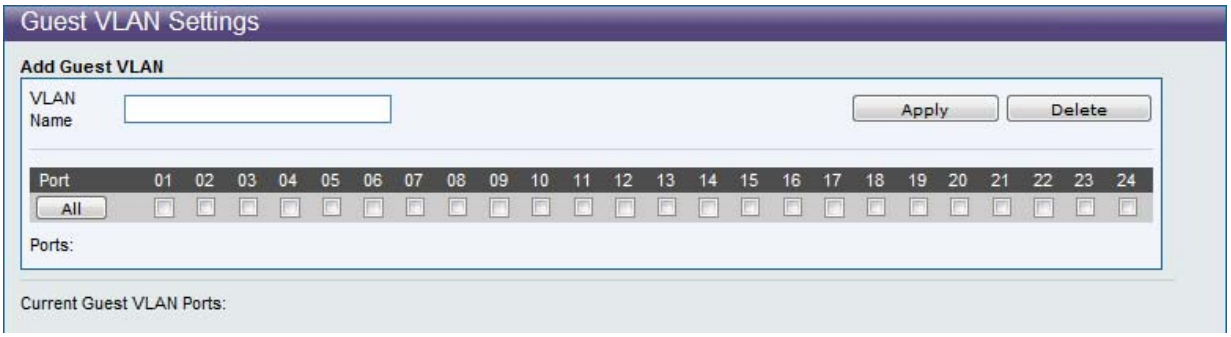
2 A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.

3 Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.

Remember, to set an 802.1X guest VLAN, the user must first configure a normal VLAN, which can be enabled here for guest VLAN status. Only one VLAN may be assigned as the 802.1X guest VLAN.

To view this window, click **Security > 802.1X > Guest VLAN Settings** as shown below:

Figure 207: Guest VLAN Settings window


Guest VLAN Settings
Add Guest VLAN
VLAN Name
Apply
Delete
Port 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
All
Ports:
Current Guest VLAN Ports:

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as an 802.1X guest VLAN.
Port	Set the ports to be enabled for the 802.1X guest VLAN. Click the **All** button to select all the ports.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry based on the information entered.

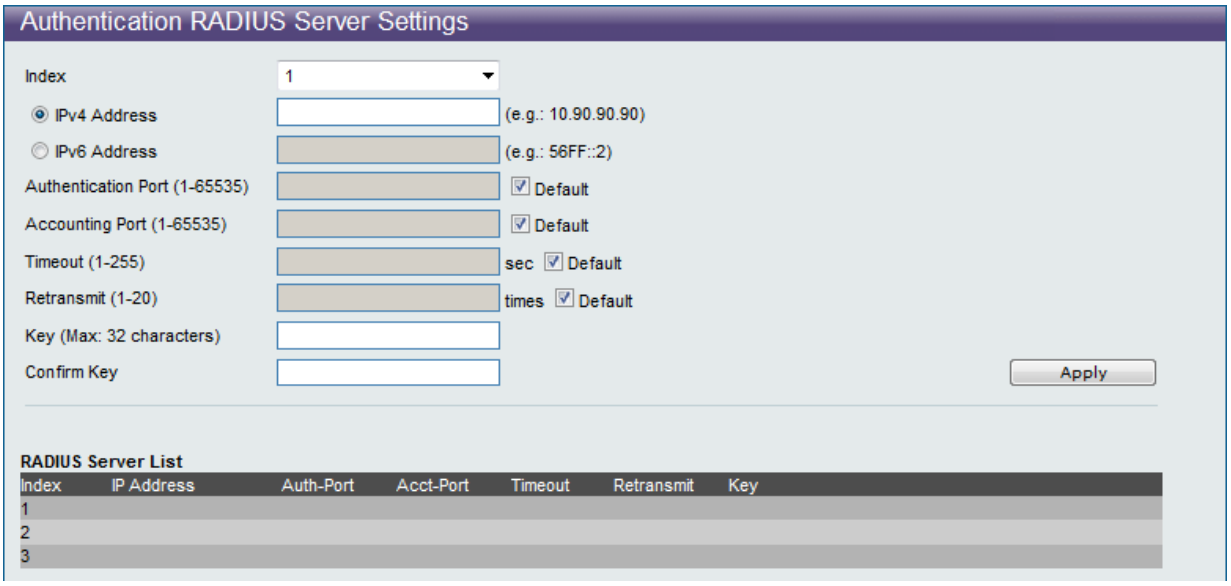
RADIUS

Authentication RADIUS Server Settings

The RADIUS feature of the Switch allows the user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

To view this window, click **Security > RADIUS > Authentication RADIUS Server Settings** as shown below:

Figure 208: Authentication RADIUS Server Settings window



The fields that can be configured are described below:

Parameter	Description
Index	Choose the desired RADIUS server to configure: *1, 2* or *3* and select the IPv4 Address.
Server IP	Set the RADIUS server IP address.
IPv4 Address	Set the RADIUS server IP address.
IPv6 Address	Set the RADIUS server IPv6 address.
Authentication Port	Set the RADIUS authentic server(s) UDP port which is used to transmit RADIUS data between the Switch and the RADIUS server. The default port is *1812*.
Accounting Port	Set the RADIUS account server(s) UDP port which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The default port is *1813*.
Timeout	Set the RADIUS server age-out, in seconds.
Retransmit	Set the RADIUS server retransmit time, in times.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the key the same as that of the RADIUS server.

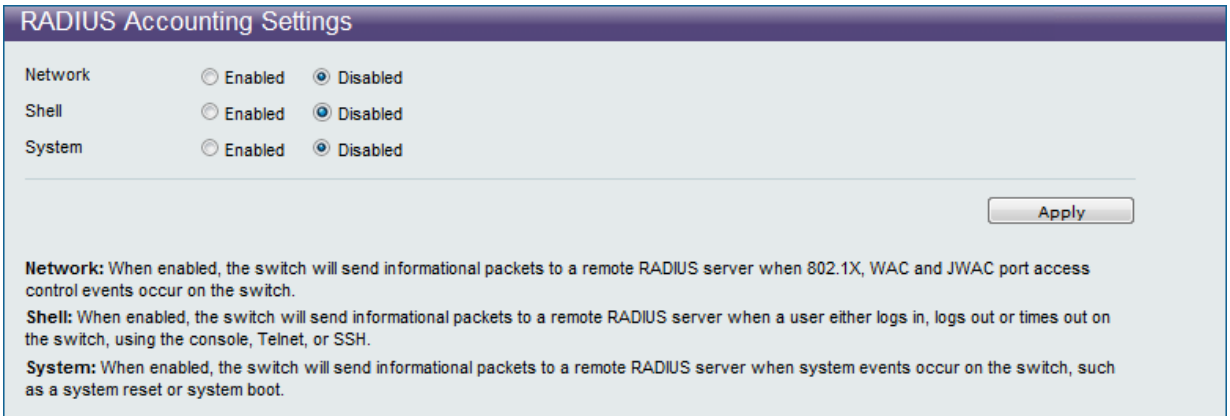
Click the **Apply** button to accept the changes made.

RADIUS Accounting Settings

Users can configure the state of the specified RADIUS accounting service.

To view this window, click **Security > RADIUS > RADIUS Accounting Settings** as shown below:

Figure 209: RADIUS Accounting Settings window


RADIUS Accounting Settings
Network
Enabled
Disabled
Shell
Enabled
Disabled
System
Enabled
Disabled
Apply
Network: When enabled, the switch will send informational packets to a remote RADIUS server when 802.1X, WAC and JWAC port access control events occur on the switch.
Shell: When enabled, the switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the switch, using the console, Telnet, or SSH.
System: When enabled, the switch will send informational packets to a remote RADIUS server when system events occur on the switch, such as a system reset or system boot.

The fields that can be configured are described below:

Parameter	Description
Network	When enabled, the Switch will send informational packets to a remote RADIUS server when 802.1X and WAC port access control events occur on the Switch.
Shell	When enabled, the Switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the Switch, using the console, Telnet, or SSH.
System	When enabled, the Switch will send informational packets to a remote RADIUS server when system events occur on the Switch, such as a system reset or system boot.

Click the **Apply** button to accept the changes made.

RADIUS Authentication

Users can display information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

To view this window, click **Security > RADIUS > RADIUS Authentication** as shown below:

Figure 210: RAIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The fields that can be configured are described below:

Parameter	Description
InvalidServerAddr	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client.
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddr	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetrans	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.

Parameter	Description
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

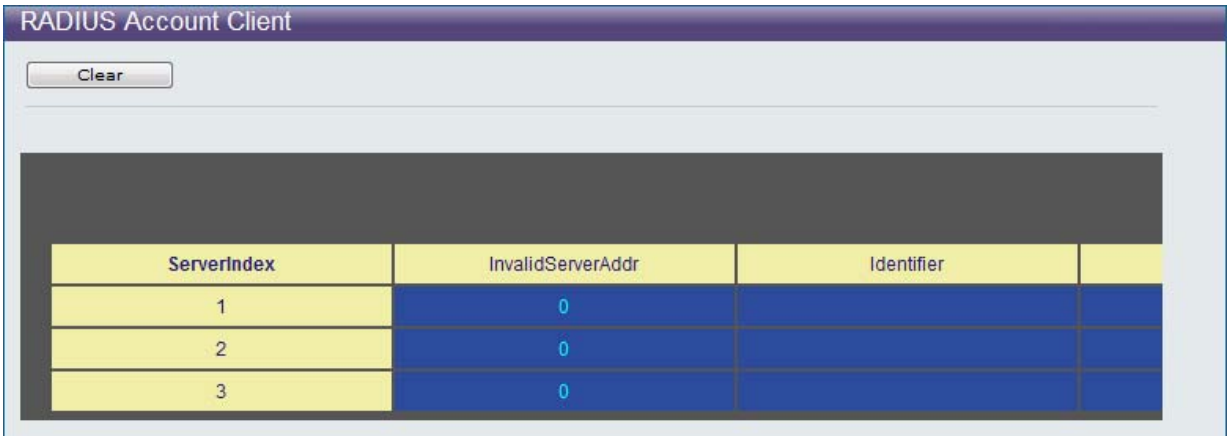
Click the **Clear** button to clear the current statistics shown.

RADIUS Account Client

Users can display managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view this window, click **Security > RADIUS > RADIUS Account Client** as shown below:

Figure 211: RADIUS Account Client window



The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

The fields that can be configured are described below:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
InvalidServerAddr	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS accounting client.

Parameter	Description
ServerAddr	The IP address of the RADIUS authentication server referred to in this table entry.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Click the **Clear** button to clear the current statistics shown.

MAC-based Access Control (MAC)

MAC-based access control is a method to authenticate and authorize access using either a port or host. For port-based MAC-based access control, the method decides port access rights, while for host-based MAC-based access control, the method determines the MAC access rights.

A MAC user must be authenticated before being granted access to a network. Both local authentication and remote RADIUS server authentication methods are supported. In MAC-based access control, MAC user information in a local database or a RADIUS server database is searched for authentication. Following the authentication result, users achieve different levels of authorization.

Notes about MAC-based Access Control

There are certain limitations and regulations regarding MAC-based access control:

1 Once this feature is enabled for a port, the Switch will clear the FDB of that port.

2 If a port is granted clearance for a MAC address in a VLAN that is not a Guest VLAN, other MAC addresses on that port must be authenticated for access and otherwise will be blocked by the Switch.

3 Ports that have been enabled for Link Aggregation and Port Security cannot be enabled for MAC-based Authentication.

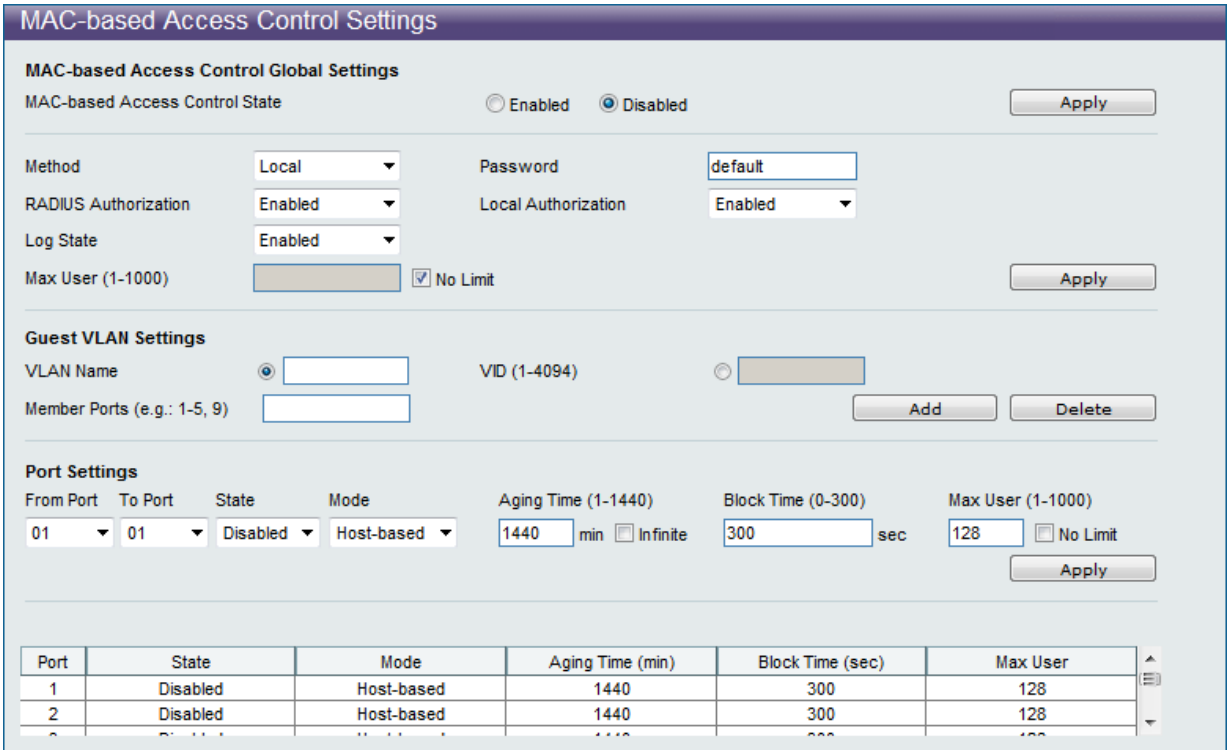
4 Ports that have been enabled for GVRP cannot be enabled for Guest VLAN.

MAC-based Access Control Settings

This window is used to set the parameters for the MAC-based access control function on the Switch. The user can set the running state, method of authentication, RADIUS password, view the Guest VLAN configuration to be associated with the MAC-based access control function of the Switch, and configure ports to be enabled or disabled for the MAC-based access control feature of the Switch. Please remember, ports enabled for certain other features, listed previously, and cannot be enabled for MAC-based access control.

To view this window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings** as shown below:

Figure 212: MAC-based Access Control Settings window



The fields that can be configured are described below:

Parameter	Description
MAC-based Access Control State	Toggle to globally enable or disable the MAC-based access control function on the Switch.
Method	Use this drop-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: *Local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based access control. This MAC address list can be configured in the MAC-based access control Local Database Settings window. *RADIUS* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based access control. Remember, the MAC list must be previously set on the RADIUS server.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.
RADIUS Authorization	Use the drop-down menu to enable or disable the use of RADIUS Authorization.
Local Authorization	Use the drop-down menu to enable or disable the use of Local Authorization.
Log State	Use the drop-down menu to enable or disable log state.
Max User	Enter the maximum amount of users of the Switch.
VLAN Name	Enter the name of the previously configured Guest VLAN being used for this function.
VID	Click the radio button and enter a Guest VLAN ID.
Member Ports	Enter the list of ports that have been configured for the Guest VLAN.
From Port	The beginning port of a range of ports to be configured for MAC-based access control.
To Port	The ending port of a range of ports to be configured for MAC-based access control.
State	Use this drop-down menu to enable or disable MAC-based access control on the port or range of ports selected in the Port Settings section of this window.
Mode	Toggle between *Port-based* and *Host-based*.
Aging Time (1-1440)	Enter a value between *1* and *1440* minutes. The default is *1440*. To set this value to have no aging time, select the **Infinite** option.
Block Time (0-300)	Enter a value between *1* and *300* seconds. The default is *300*.
Max User (1-1000)	Enter the maximum user used for this configuration. When **No Limit** is selected, there will be no user limit applied to this rule.

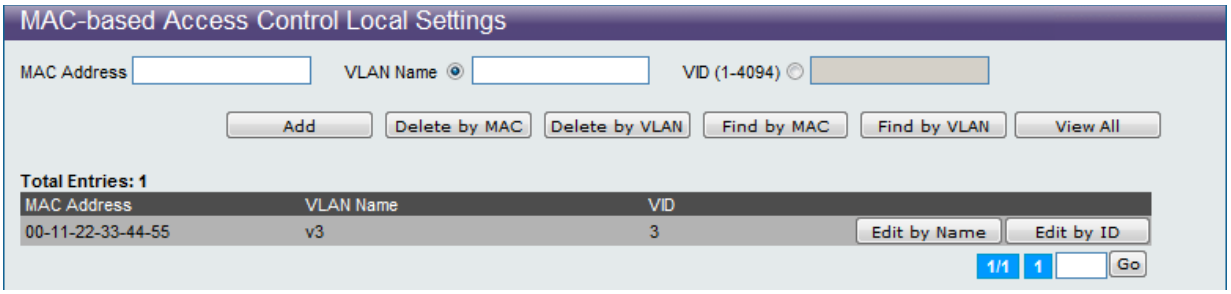
Click the **Apply** button to accept the changes made for each individual section.

MAC-based Access Control Local Settings

Users can set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this window, it will be placed in the VLAN associated with it here. The Switch administrator may enter up to 128 MAC addresses to be authenticated using the local method configured here.

To view this window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings** as shown below:

Figure 213: MAC-based Access Control Local Settings window



The fields that can be configured are described below:

Parameter	Description
MAC address	Enter the MAC address that will be added to the local authentication list here.
VLAN Name	Enter the VLAN name of the corresponding MAC address here.
VID (1-4094)	Enter the VLAN ID of the corresponding MAC address here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete by MAC** button to remove the specific entry based on the MAC address entered.

Click the **Delete by VLAN** button to remove the specific entry based on the VLAN name or ID entered.

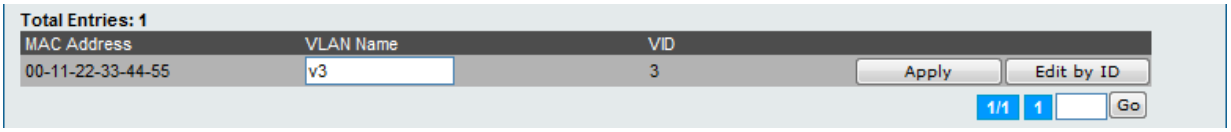
Click the **Find by MAC** button to locate a specific entry based on the MAC address entered.

Click the **Find by VLAN** button to locate a specific entry based on the VLAN name or ID entered.

Click the **View All** button to display all the existing entries.

To change the selected MAC address' VLAN Name, the user can click the **Edit by Name** button.

Figure 214: MAC-based Access Control Local Settings – Edit by Name window



To change the selected MAC address' VID value, the user can click the **Edit by ID** button.

Figure 215: MAC-based Access Control Local Settings – Edit by ID window

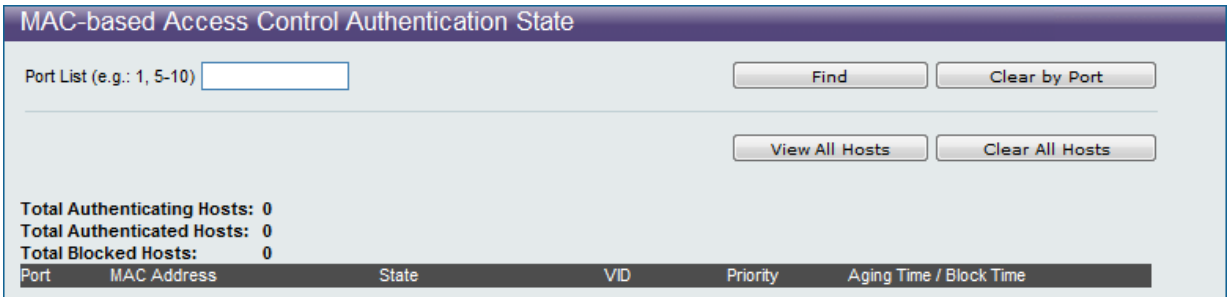
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MAC-based Access Control Authentication State

Users can display MAC-based access control Authentication State information.

To view this window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State** as shown below:

Figure 216: MAC-based Access Control Authentication State window



To display MAC-based access control Authentication State information, enter a port number in the space provided and then click the **Find** button.

Click the **Clear by Port** button to clear all the information linked to the port number entered.

Click the **View All Hosts** button to display all the existing hosts.

Click the **Clear All hosts** button to clear out all the existing hosts.

Web-based Access Control (WAC)

Web-based Authentication Login is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol. The Switch enters the authenticating stage when users attempt to browse Web pages through a Web browser. When the Switch detects HTTP or HTTPS packets and this port is un-authenticated, the Switch will launch a pop-up user name and password window to query users. Users are not able to access the Internet until the authentication process is passed.

The Switch can be the authentication server itself and do the authentication based on a local database, or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server. The client user initiates the authentication process of WAC by attempting to gain Web access.

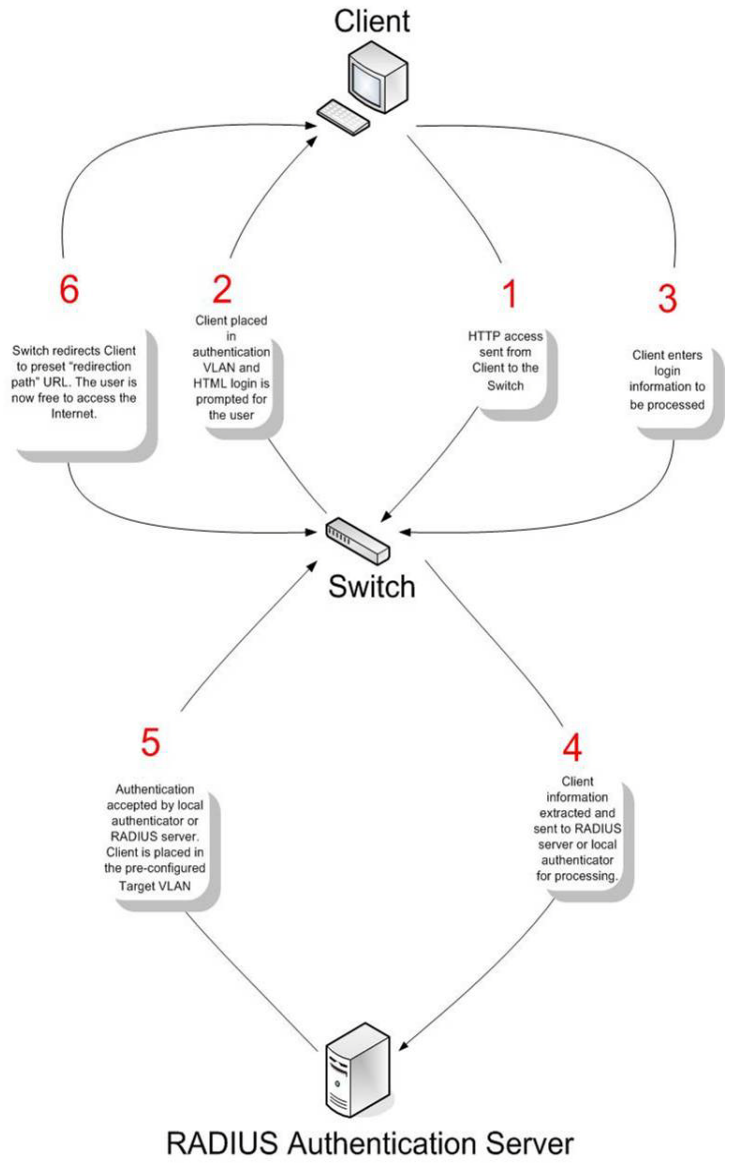
Extreme's implementation of WAC uses a virtual IP that is exclusively used by the WAC function and is not known by any other modules of the Switch. In fact, to avoid affecting a Switch's other features, WAC will only use a virtual IP address to communicate with hosts. Thus, all authentication requests must be sent to a virtual IP address but not to the IP address of the Switch's physical interface.

Virtual IP works like this, when a host PC communicates with the WAC Switch through a virtual IP, the virtual IP is transformed into the physical IPIF (IP interface) address of the Switch to make the communication possible. The host PC and other servers' IP configurations do not depend on the virtual IP of WAC. The virtual IP does not respond to any ICMP packets or ARP requests, which means it is not allowed to configure a virtual IP on the same subnet as the Switch's IPIF (IP interface) or the same subnet as the host PCs' subnet.

As all packets to a virtual IP from authenticated and authenticating hosts will be trapped to the Switch's CPU, if the virtual IP is the same as other servers or PCs, the hosts on the WAC-enabled ports cannot communicate with the server or PC which really own the IP address. If the hosts need to access the server or PC, the virtual IP cannot be the same as the one of the server or PC. If a host PC uses a proxy to access the Web, to make the authentication work properly the user of the PC should add the virtual IP to the exception of the proxy configuration. Whether or not a virtual IP is specified, users can access the WAC pages through the Switch's system IP. When a virtual IP is not specified, the authenticating Web request will be redirected to the Switch's system IP.

The Switch's implementation of WAC features a user-defined port number that allows the configuration of the TCP port for either the HTTP or HTTPS protocols. This TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to the CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80 and the default port number for HTTPS is 443. If no protocol is specified, the default protocol is HTTP.

The following diagram illustrates the basic six steps all parties go through in a successful Web Authentication process:


Client
6
Switch redirects Client to preset "redirection path" URL. The user is now free to access the Internet.
2
Client placed in authentication VLAN and HTML login is prompted for the user
1
HTTP access sent from Client to the Switch
3
Client enters login information to be processed
Switch
5
Authentication accepted by local authenticator or RADIUS server. Client is placed in the pre-configured Target VLAN
4
Client information extracted and sent to RADIUS server or local authenticator for processing.
RADIUS Authentication Server

Conditions and Limitations

1 If the client is utilizing DHCP to attain an IP address, the authentication VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.

2 Certain functions exist on the Switch that will filter HTTP packets, such as the Access Profile function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.

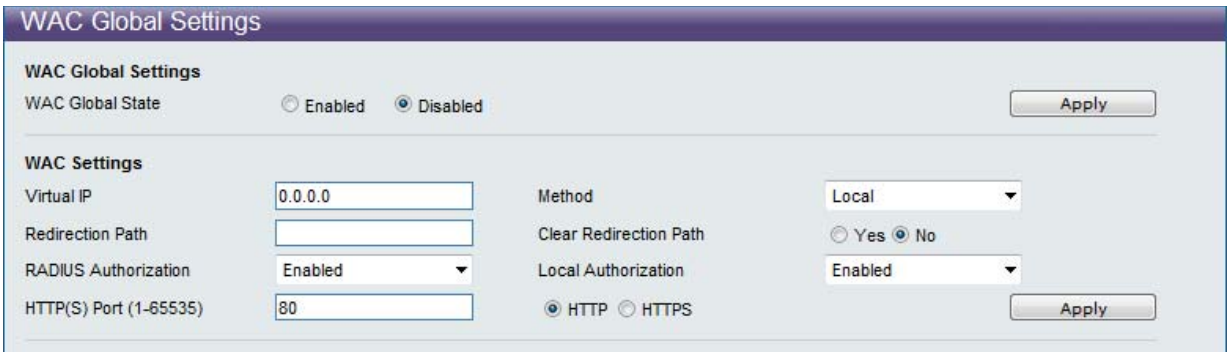
3 If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling Web Authentication on the Switch.

WAC Global Settings

Users can configure the Switch for the Web-based access control function.

To view this window, click **Security > Web-based Access Control (WAC) > WAC Global Settings** as shown below:

Figure 217: WAC Global Settings window



The fields that can be configured are described below:

Parameter	Description
WAC Global State	Use this selection menu to either enable or disable the Web Authentication on the Switch.
Virtual IP	Enter a virtual IP address. This address is only used by WAC and is not known by any other modules of the Switch.
Method	Use this drop-down menu to choose the authenticator for Web-based Access Control. The user may choose: *Local* – Choose this parameter to use the local authentication method of the Switch as the authenticating method for users trying to access the network via the switch. This is, in fact, the username and password to access the Switch configured using the WAC User Settings window (**Security** > **Web-based Access Control** > **WAC User Settings**) seen below. *RADIUS* – Choose this parameter to use a remote RADIUS server as the authenticating method for users trying to access the network via the switch. This RADIUS server must have already been pre-assigned by the administrator using the Authentication RADIUS Server Settings window (**Security** > **RADIUS** > **Authentication RADIUS Server Settings**).
Redirection Path	Enter the URL of the website that authenticated users placed in the VLAN are directed to once authenticated.

Parameter	Description
Clear Redirection Path	The user can enable or disable this option to clear the redirection path.
RADIUS Authorization	The user can enable or disable this option to enable RADIUS Authorization or not.
Local Authorization	The user can enable or disable this option to enable Local Authorization or not.
HTTP(S) Port (1-65535)	Enter a HTTP port number. Port *80* is the default. *HTTP* – Specifies that the TCP port will run the WAC HTTP protocol. The default value is 80. HTTP port cannot run at TCP port 443. *HTTPS* – Specifies that the TCP port will run the WAC HTTPS protocol. The default value is 443. HTTPS cannot run at TCP port 80.

Click the **Apply** button to accept the changes made for each individual section.

NOTE

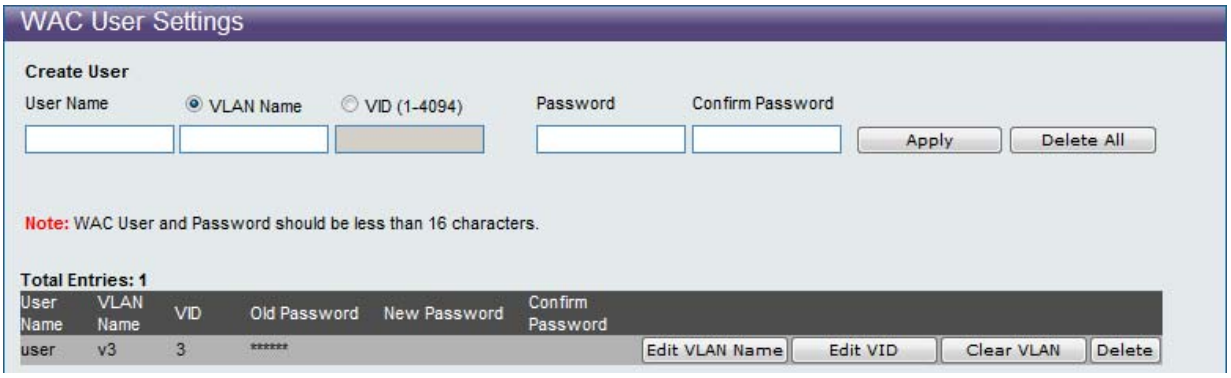
A successful authentication should direct the client to the stated web page. If the client does not reach this web page, yet does not receive a **Fail!** Message, the client will already be authenticated and therefore should refresh the current browser window or attempt to open a different web page.

WAC User Settings

Users can view and set local database user accounts for Web authentication.

To view this window, click **Security > Web-based Access Control (WAC) > WAC User Settings** as shown below:

Figure 218: WAC User Settings window



The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user name of up to 15 alphanumeric characters of the guest wishing to access the Web through this process. This field is for administrators who have selected *Local* as their Web-based authenticator.
VLAN Name	Click the button and enter a VLAN Name in this field.

Parameter	Description
VID (1-4094)	Click the button and enter a VID in this field.
Password	Enter the password the administrator has chosen for the selected user. This field is case-sensitive and must be a complete alphanumeric string. This field is for administrators who have selected *Local* as their Web-based authenticator.
Confirmation	Retype the password entered in the previous field.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit VLAN Name** button to re-configure the specific entry's VLAN Name.

Click the **Edit VID** button to re-configure the specific entry's VLAN ID.

Click the **Clear VLAN** button to remove the VLAN information from the specific entry.

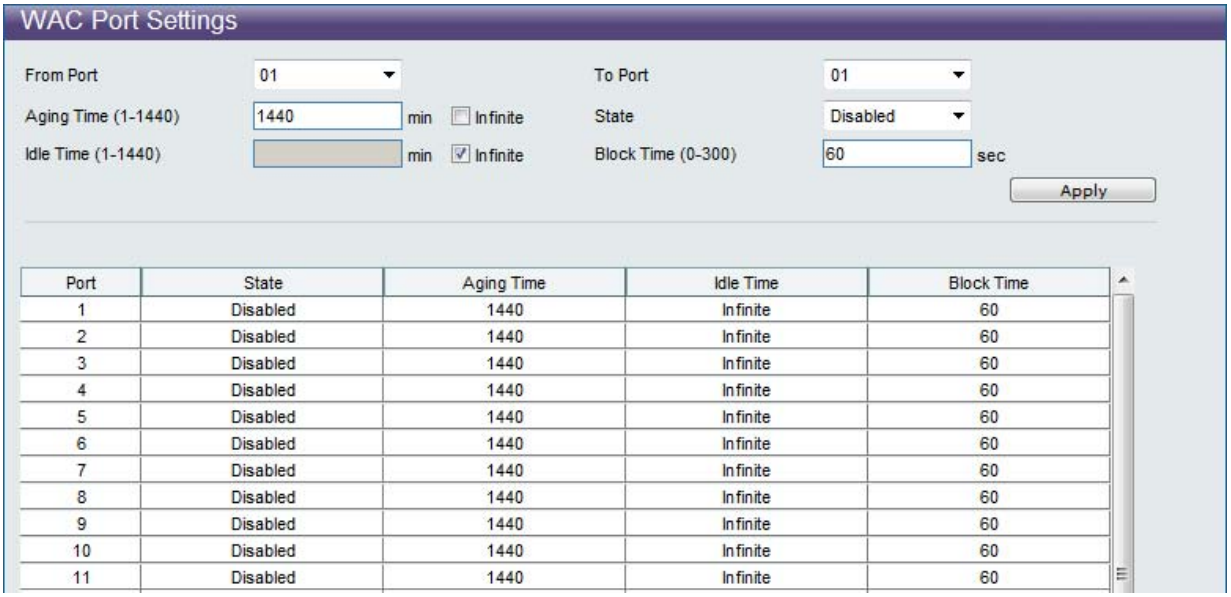
Click the **Delete** button to remove the specific entry.

WAC Port Settings

Users can view and set port configurations for Web authentication.

To view this window, click **Security > Web-based Access Control (WAC) > WAC Port Settings** as shown below:

Figure 219: WAC Port Settings window



The fields that can be configured are described below:

Parameter	Description
From Port	Use this drop-down menu to select the beginning port of a range of ports to be enabled as WAC ports.
To Port	Use this drop-down menu to select the ending port of a range of ports to be enabled as WAC ports.
Aging Time (1-1440)	This parameter specifies the time period during which an authenticated host will remain in the authenticated state. Enter a value between *1*and *1440* minutes. Tick the **Infinite** check box to indicate the authenticated host will never age out on the port. The default value is *1440* minutes (24 hours).
State	Use this drop-down menu to enable the configured ports as WAC ports.
Idle Time (1-1440)	If there is no traffic during the Idle Time parameter, the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. Tick the **Infinite** check box to indicate the Idle state of the authenticated host on the port will never be checked. The default value is *infinite*.
Block Time (0-300)	This parameter is the period of time a host will be blocked if it fails to pass authentication. Enter a value between *0* and *300* seconds. The default value is *60* seconds.

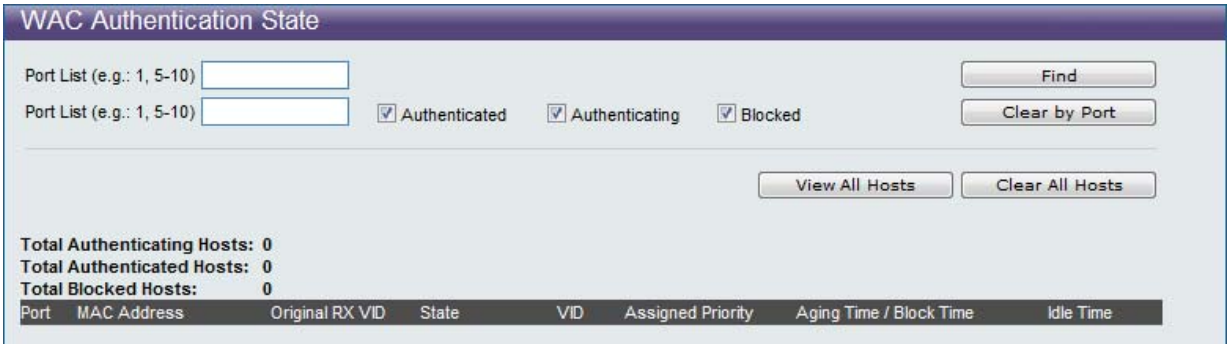
Click the **Apply** button to accept the changes made.

WAC Authentication State

Users can view and delete the hosts for Web authentication.

To view this window, click **Security > Web-based Access Control (WAC) > WAC Authentication State a**s shown below:

Figure 220: WAC Authentication State window



The fields that can be configured are described below:

Parameter	Description
Port List	Enter the desired range of ports and tick the appropriate check box(s), Authenticated, Authenticating, and Blocked.
Authenticated	Tick this check box to clear all authenticated users for a port.
Authenticating	Tick this check box to clear all authenticating users for a port.
Blocked	Tick this check box to clear all blocked users for a port.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear by Port** button to remove entry based on the port list entered.

Click the **View All Hosts** button to display all the existing entries.

Click the **Clear All Hosts** button to remove all the entries listed.

Compound Authentication

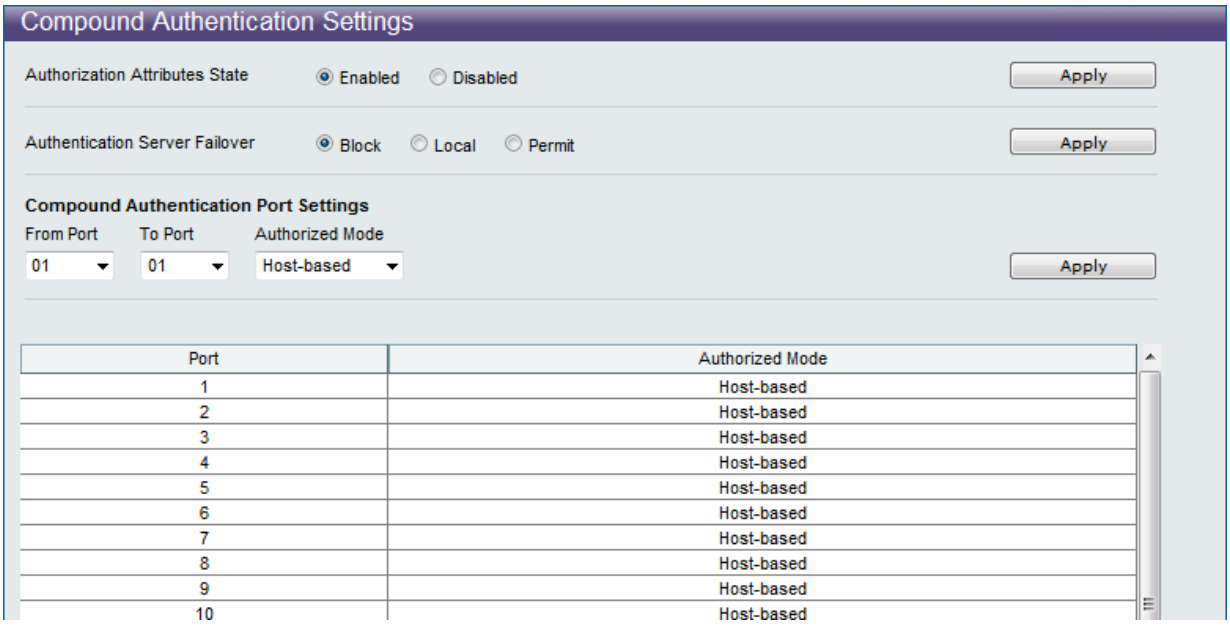
Compound Authentication settings allows for multiple authentication to be supported on the Switch.

Compound Authentication Settings

Users can configure Authorization Network State Settings and compound authentication methods for a port or ports on the Switch.

To view this window, click **Security > Compound Authentication > Compound Authentication Settings** as shown below:

Figure 221: Compound Authentication Settings window



The fields that can be configured are described below:

Parameter	Description
Authorization Network State	Click the radio buttons to enable of disable the Authorization Network State.

Parameter	Description
Authentication Server Failover	Click the radio buttons to configure the authentication server failover function.
	Local. The switch will resort to using the local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated, otherwise, it authenticated.
	Permit. The client is always regarded as authenticated. If guest VLAN is enabled, clients will stay on the guest VLAN, otherwise, they will stay on the original VLAN.
	Block (default setting). The client is always regarded as un-authenticated.
From Port	Use this drop-down menu to select the beginning port of a range of ports to be enabled as compound authentication ports.
To Port	Use this drop-down menu to select the ending port of a range of ports to be enabled as compound authentication ports.
Authorized Mode	Toggle between *Host-based* and *Port-based*. When *Port-based* is selected, if one of the attached hosts passes the authentication, all hosts on the same port will be granted access to the network. If the user fails the authorization, this port will keep trying the next authentication method. When *Host-based* is selected, users are authenticated individually.

Click the **Apply** button to accept the changes made for each individual section.

Port Security

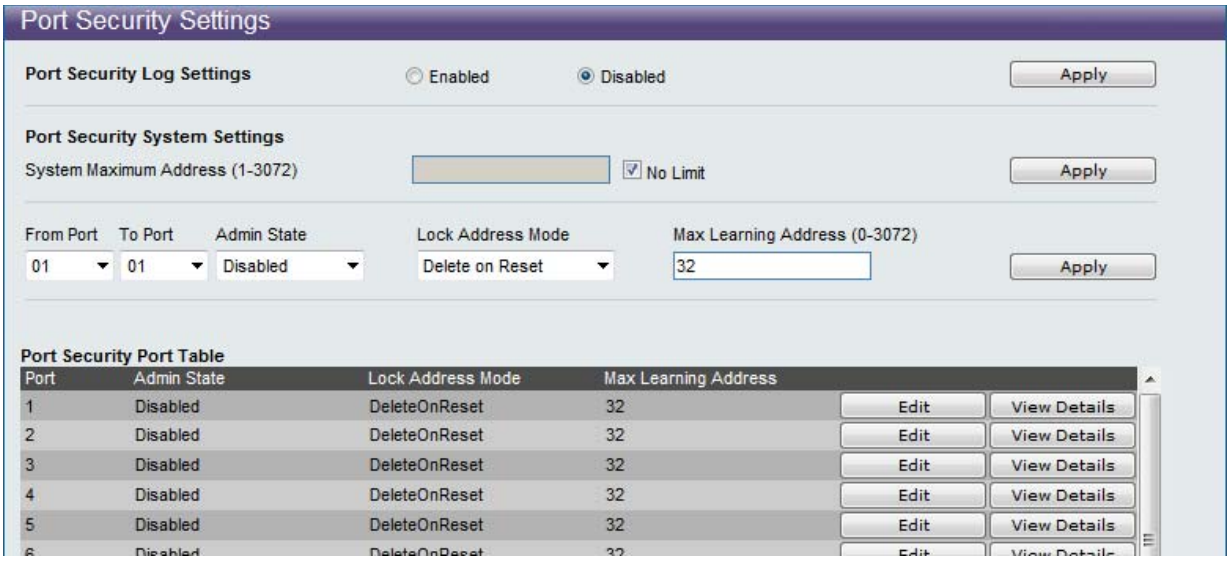
Port Security Settings

A given port's (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port lock is enabled. The port can be locked by changing the **Admin State** pull-down menu to *Enabled* and clicking **Apply**.

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view this window, click **Security > Port Security > Port Security Settings** as shown below:

Figure 222: Port Security Settings window



The fields that can be configured are described below:

Parameter	Description
Port Security Log Settings	Use the radio button to enable or disable Port Security Logs on the Switch.
System Max Address	Enter the system maximum address.
From Port	The beginning port of a consecutive group of ports to be configured.
To Port	The ending port of a consecutive group of ports to be configured.
Admin State	Use the pull-down menu to enable or disable Port Security (locked MAC address table for the selected ports).
Lock Address Mode	This pull-down menu allows the option of how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: *Permanent* – The locked addresses will only age out after the Switch has been reset. *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset or rebooted.
Max Learning Address	Specify the maximum value of port security entries that can be learned on this port.

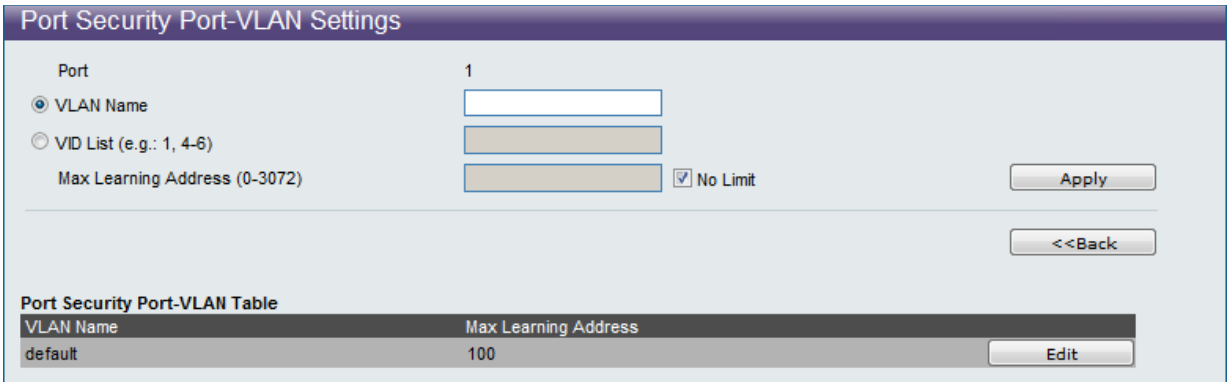
Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.

Click the **View Detail** button to display the information of the specific entry.

After clicking the **View Detail** button, the following page will appear:

Figure 223: Port Security Port-VLAN Settings window



Click the **Apply** button to accept the changes made.

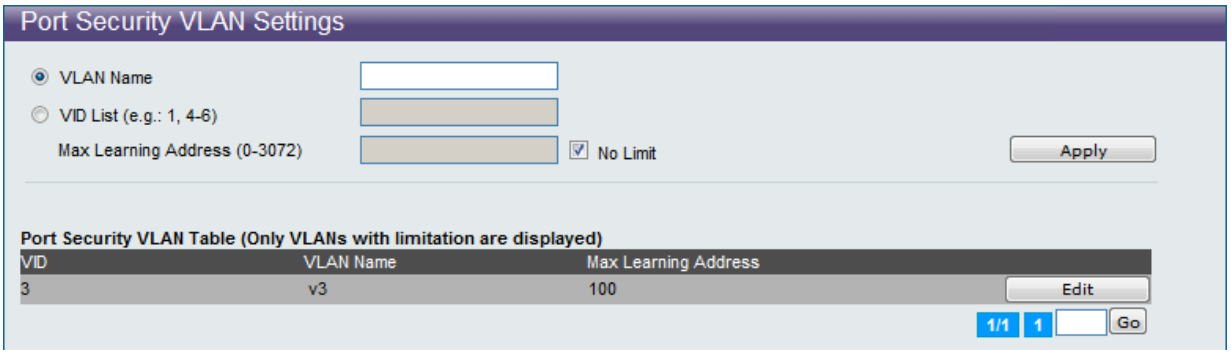
Click the **<<Back** button to discard the changes made and return to the previous page.

Port Security VLAN Settings

Users can configure the maximum number of port-security entries that can be learned on a specific VLAN.

To view this window, click **Security > Port Security > Port Security VLAN Settings** as shown below:

Figure 224: Port Security VLAN Settings window



The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter the VLAN Name.
VID List	Specify a list of the VLAN be VLAN ID.
Max Learning Address	Specify the maximum number of port-security entries that can be learned by this VLAN.

Click the **Apply** button to accept the changes made.

Port Security Entries

Users can remove an entry from the port security entries learned by the Switch and entered into the forwarding database.

To view this window, click **Security > Port Security > Port Security Entries** as shown below:

Figure 225: Port Security Entries window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
VID List	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
Port List	Enter the port number or list here to be used for the port security entry search. When **All** is selected, all the ports configured will be displayed.
MAC Address	The MAC address of the entry in the forwarding database table that has been permanently learned by the Switch.
Lock Mode	The type of MAC address in the forwarding database table.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the entries based on the information entered.

Click the **Show All** button to display all the existing entries.

Click the **Clear All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

BPDU Attack Protection

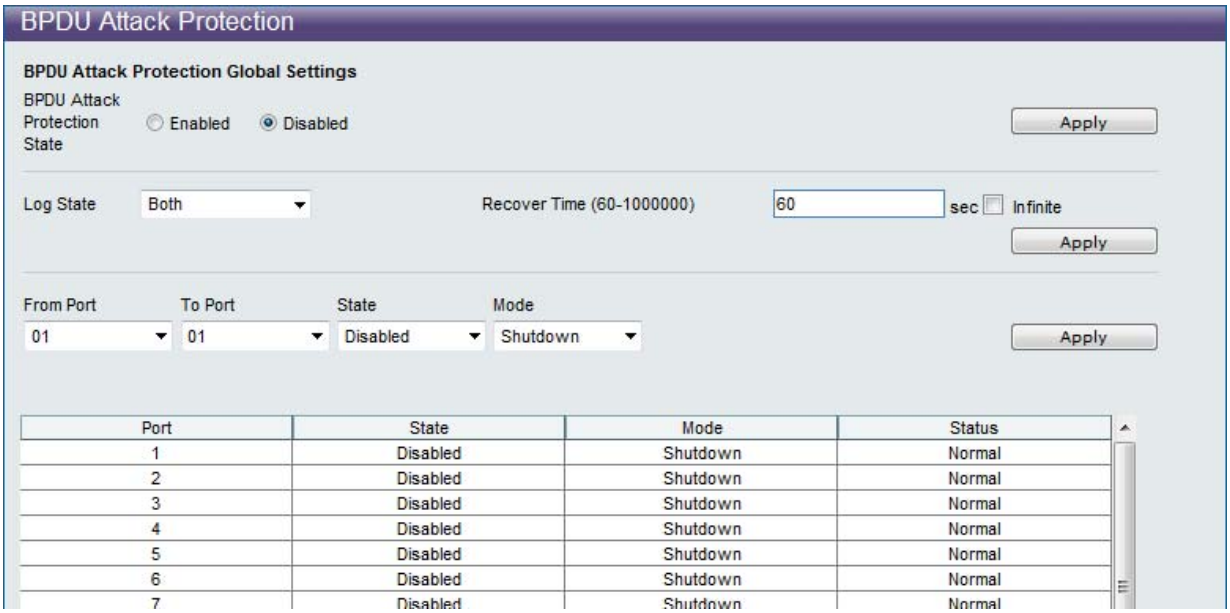
This page is used to configure the BPDU protection function for the ports on the switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter an under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on the STP-disabled port.

BPDU protection has a higher priority than the FBPDU setting configured by configure STP command in the determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has a higher priority than the BPDU tunnel port setting in determination of BPDU handling. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU.

To view this window, click **Security > BPDU Attack Protection** as shown below:

Figure 226: BPDU Attack Protection window



The fields that can be configured are described below:

Parameter	Description
BPDU Attack Protection State	Click the radio buttons to enable or disable the BPDU Attack Protection state.
Log State	Specify when a log entry will be sent. Options to choose from are **None**, **Attack Detected**, **Attack Cleared** or **Both**.
Recover Time	Specify the BPDU protection Auto-Recovery timer. The default value of the recovery timer is 60.
From Port / To Port	Select a range of ports to use for this configuration.
State	Use the drop-down menu to enable or disable the protection mode for a specific port.
Mode	Specify the BPDU protection mode. The default mode is shutdown.
	Drop – Drop all received BPDU packets when the port enters under attack state.
	Block – Drop all packets (include BPDU and normal packets) when the port enters under attack state.
	Shutdown – Shut down the port when the port enters under attack state.

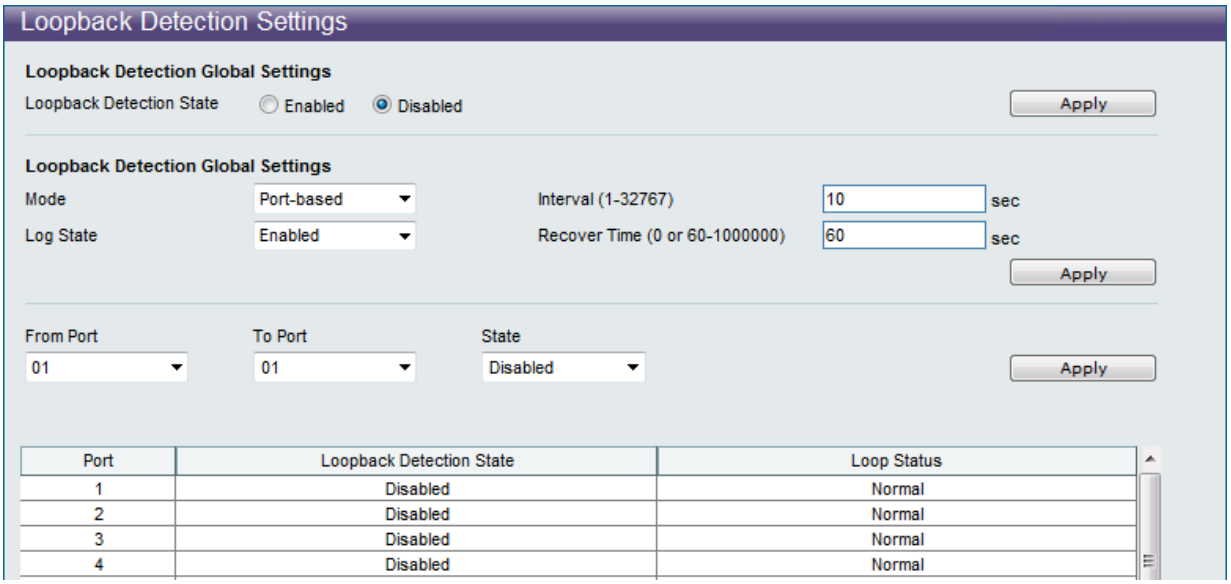
Click the **Apply** button to accept the changes made for each individual section.

Loopback Detection Settings

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port, this signifies a loop on the network. The Switch will automatically block the port and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the pull-down menu.

To view this window, click **Security > Loopback Detection Settings** as shown below:

Figure 227: Loopback Detection Settings window



The fields that can be configured are described below:

Parameter	Description
LBD State	Use the radio button to enable or disable loopback detection. The default is Disabled.
Mode	Use the drop-down menu to select *Port-based.*
Log State	Specifies the state of the log for loopback detection.
Interval (1-32767)	The time interval (in seconds) that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The valid range is from *1* to *32767* seconds. The default setting is *10* seconds.
Recover Time (0 or 60-1000000)	Time allowed (in seconds) for recovery when a Loopback is detected. The Loop-detect Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loop-detect Recover Time. The default is *60* seconds.
From Port	Use the drop-down menu to select a beginning port number.
To Port	Use the drop-down menu to select an ending port number.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled*.

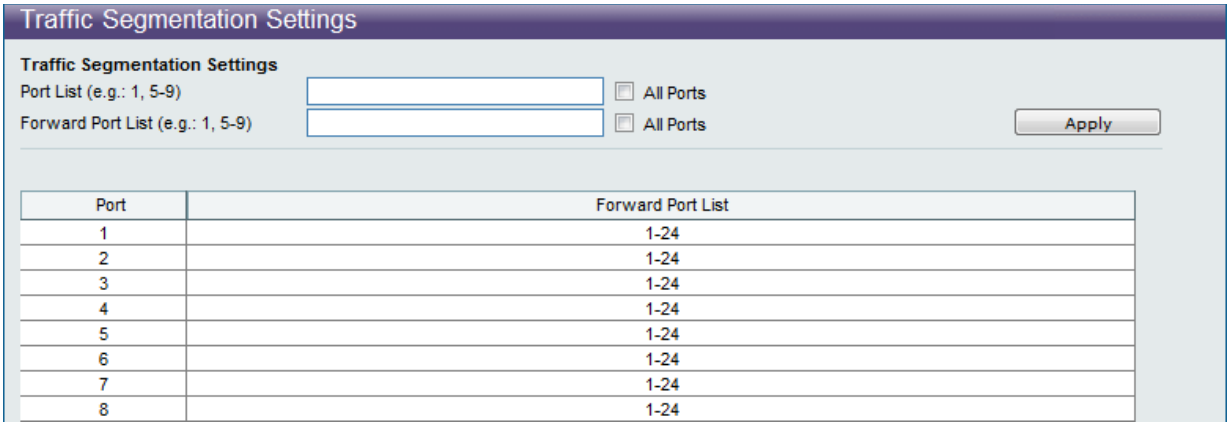
Click the **Apply** button to accept the changes made for each individual section.

Traffic Segmentation Settings

Traffic segmentation is used to limit traffic flow from a single or group of ports, to a group of ports. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the master switch CPU.

To view this window, click **Security > Traffic Segmentation Settings** as shown below:

Figure 228: Traffic Segmentation Settings window



The fields that can be configured are described below:

Parameter	Description
Port List	Here the user can select the ports to be included in the traffic segmentation setup.
Forward Port List	Here the user can select the ports to be included in the traffic segmentation setup by simply ticking the corresponding port's tick box. Click the **Clear All** button to un-select all the ports for the configuration. Click the **Select All** button to select all the ports for the configuration.
Ports	Here the ports that have been selected to be included in the traffic segmentation setup will be displayed.

Click the **Apply** button to accept the changes made.

Access Authentication Control

The TACACS / XTACACS / TACACS+ / RADIUS commands allow users to secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- **TACACS** (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- **Extended TACACS (XTACACS)** - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- **TACACS+ (Terminal Access Controller Access Control System plus**) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

The server verifies the username and password, and the user is granted normal user privileges on the Switch.

The server will not accept the username and password and the user is denied access to the Switch.

The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the Switch.

NOTE

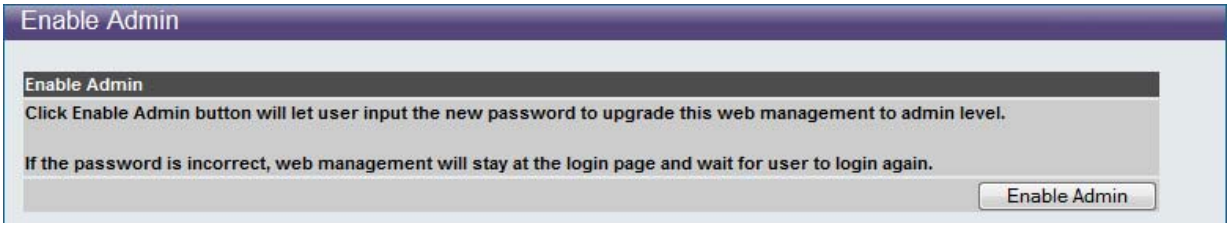
TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.

Enable Admin

Users who have logged on to the Switch on the normal user level and wish to be promoted to the administrator level can use this window. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username "enable", and a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.

To view this window, click **Security > Access Authentication Control > Enable Admin** as shown below:

Figure 229: Enable Admin window


Enable Admin
Enable Admin
Click Enable Admin button will let user input the new password to upgrade this web management to admin level.
If the password is incorrect, web management will stay at the login page and wait for user to login again.
Enable Admin

When this window appears, click the **Enable Admin** button revealing a window for the user to enter authentication (password, username), as shown below. A successful entry will promote the user to Administrator level privileges on the Switch.

Figure 230: Log-in Page

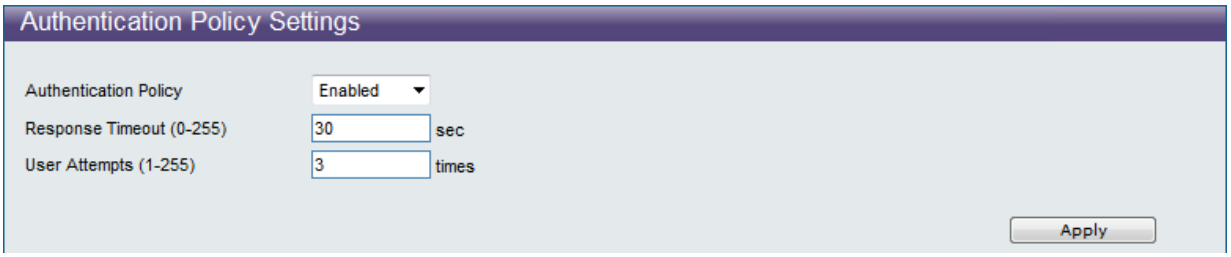
Windows Security
The server 192.168.69.123 at Welcome requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin
Password
Remember my credentials
OK
Cancel

Authentication Policy Settings

Users can enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.

To view this window, click **Security > Access Authentication Control > Authentication Policy Settings** as shown below:

Figure 231: Authentication Policy Settings window



The fields that can be configured are described below:

Parameter	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.

Parameter	Description
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

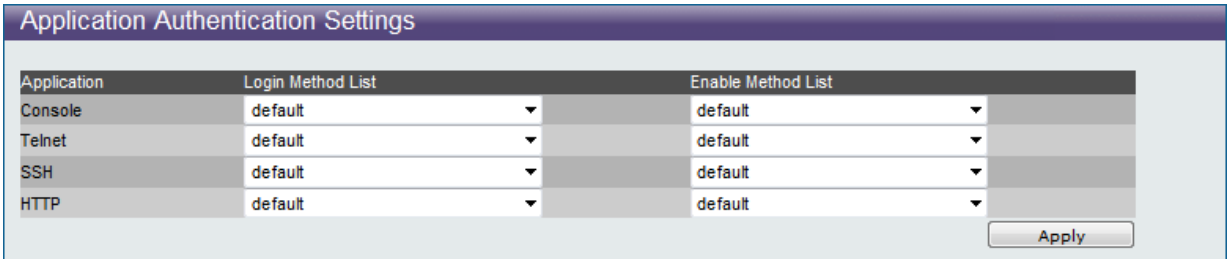
Click the **Apply** button to accept the changes made.

Application Authentication Settings

Users can configure Switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (Enable Admin**)** utilizing a previously configured method list.

To view this window, click **Security > Access Authentication Control > Application Authentication Settings** as shown below:

Figure 232: Application Authentication Settings window



The fields that can be configured are described below:

Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH, and the Web (HTTP) application.
Login Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Login Method Lists window, in this section, for more information.
Enable Method List	Using the pull-down menu, configure an application to promote user level to admin-level users utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Enable Method Lists window, in this section, for more information

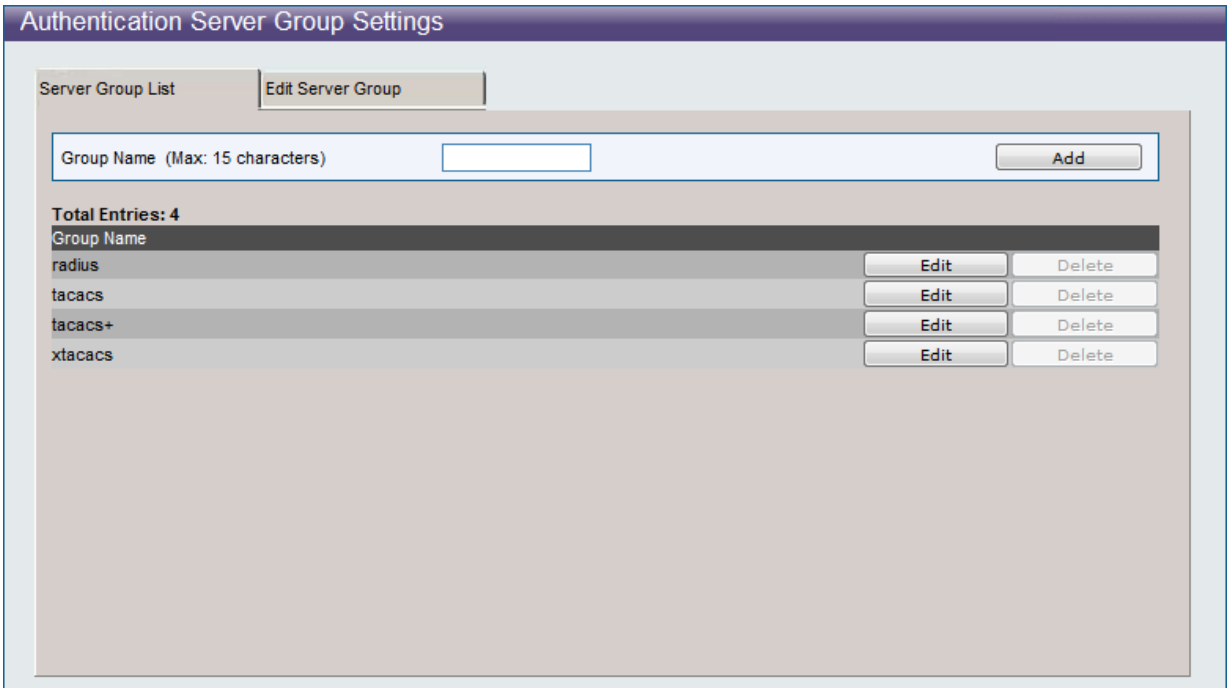
Click the **Apply** button to accept the changes made.

Authentication Server Group Settings

Users can set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

To view this window, click **Security > Access Authentication Control > Authentication Server Group Settings** as shown below:

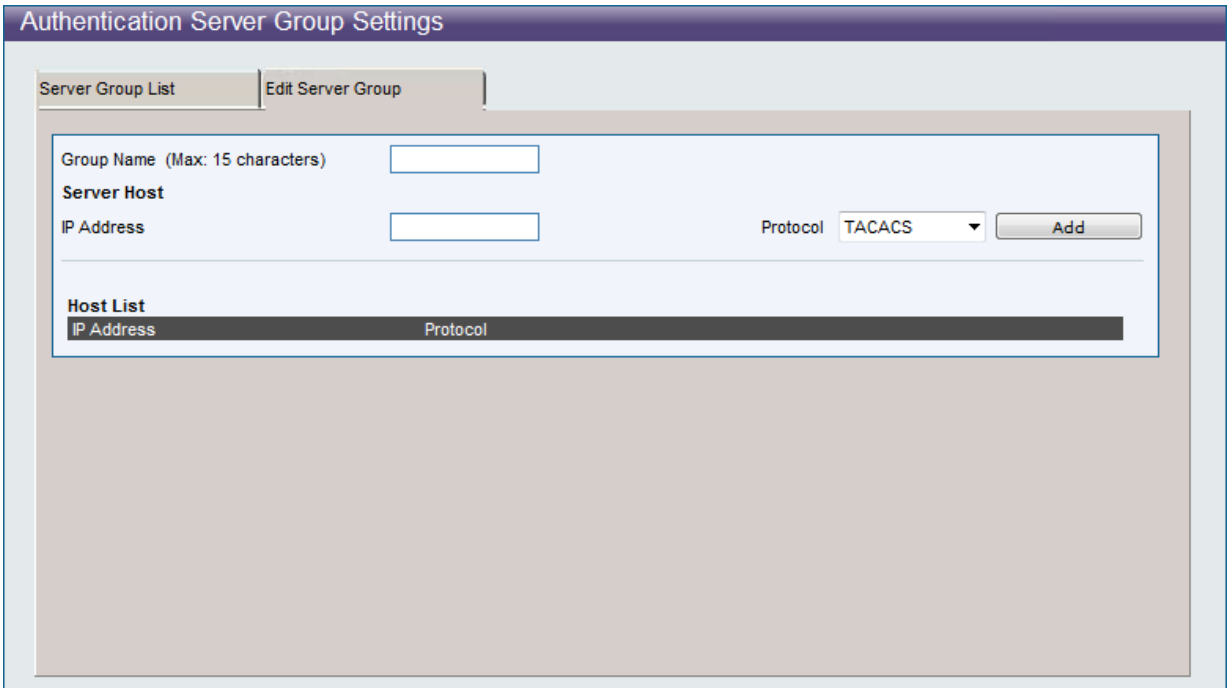
Figure 233: Authentication Server Group Settings – Server Group List window



This window displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To add a new Server Group, enter a name in the **Group Name** field and then click the **Add** button. To modify a particular group,

click the **Edit** button (or the **Edit Server Group** tab), which will then display the following **Edit Server Group** tab:

Figure 234: Authentication Server Group Settings – Edit Server Group window



To add an Authentication Server Host to the list, enter its name in the **Group Name** field, IP address in the **IP Address** field, use the drop-down menu to choose the **Protocol** associated with the IP address of the Authentication Server Host, and then click **Add** to add this Authentication Server Host to the group. The entry should appear in the Host List at the bottom of this tab.

NOTE

The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

NOTE

The three built-in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

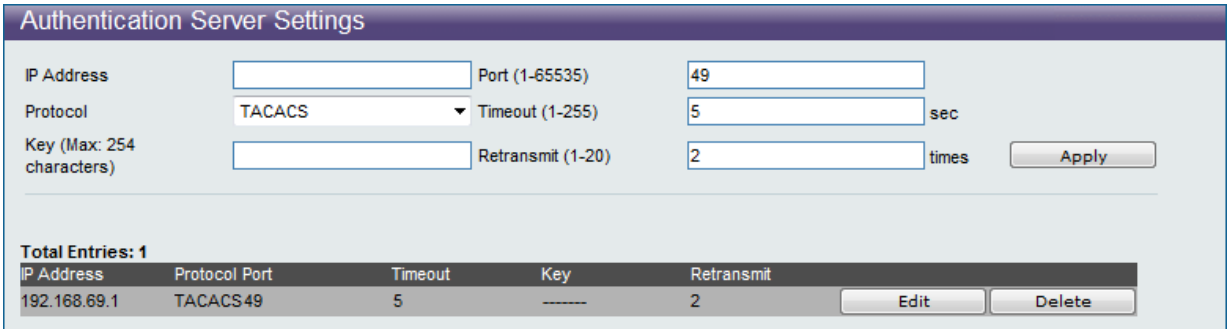
Authentication Server Settings

User-defined Authentication Server Hosts for the TACACS / XTACACS / TACACS+ / RADIUS security protocols can be set on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS / XTACACS / TACACS+ / RADIUS server host on a remote host. The TACACS / XTACACS / TACACS+ / RADIUS server host will then verify or deny the request and return the appropriate

message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS / XTACACS / TACACS+ / RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view this window, click **Security > Access Authentication Control > Authentication Server Settings** as shown below:

Figure 235: Authentication Server Settings window



The fields that can be configured are described below:

Parameter	Description
IP Address	The IP address of the remote server host to add.
Protocol	The protocol used by the server host. The user may choose one of the following: *TACACS* - Enter this parameter if the server host utilizes the TACACS protocol. *XTACACS* - Enter this parameter if the server host utilizes the XTACACS protocol. *TACACS+* - Enter this parameter if the server host utilizes the TACACS+ protocol. *RADIUS* - Enter this parameter if the server host utilizes the RADIUS protocol.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
Port (1-65535)	Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1813* for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255 sec)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.
Retransmit (1-255 times)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.

Click the **Apply** button to accept the changes made.

NOTE

More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other.

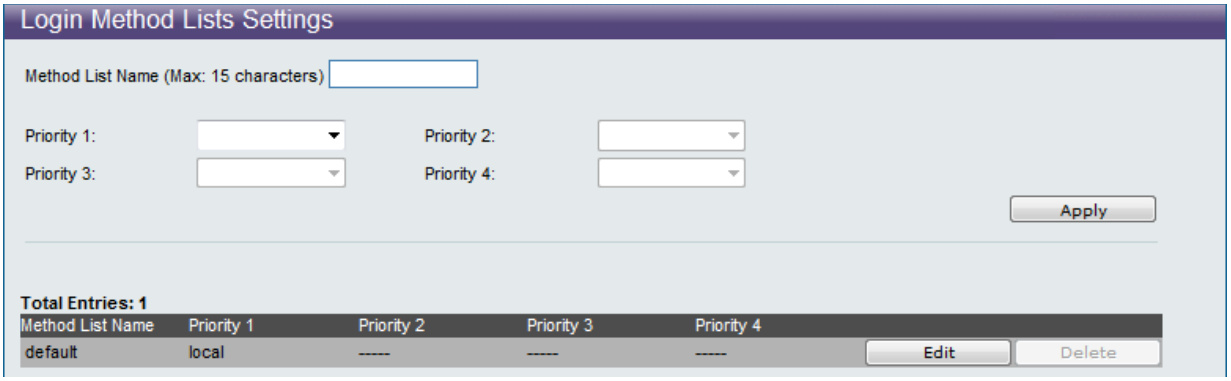
Login Method Lists Settings

User-defined or default Login Method List of authentication techniques can be configured for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS - XTACACS- local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependent on the local account privilege configured on the Switch.

Successful login using any of these techniques will give the user a "User" privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator.

To view this window, click **Security > Access Authentication Control > Login Method Lists Settings** as shown below:

Figure 236: Login Method Lists Settings window



The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the **Delete** button corresponding to the entry desired to be deleted. To modify a Login Method List, click on its corresponding **Edit** button.

The fields that can be configured are described below:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.

Parameter	Description
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *local* - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. *none* - Adding this parameter will require no authentication needed to access the Switch.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enable Method Lists Settings

Users can set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

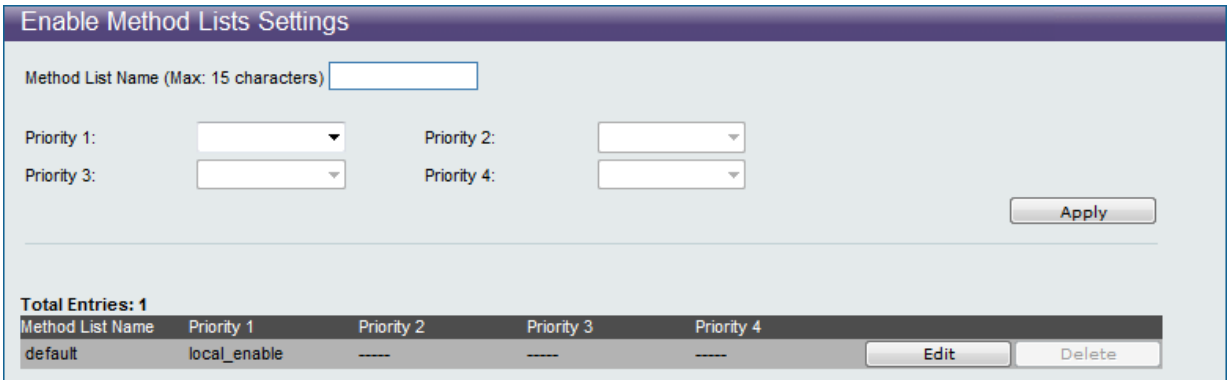
Successful authentication using any of these methods will give the user an "Admin" privilege.

NOTE

To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view this window, click **Security > Access Authentication Control > Enable method Lists Settings** as shown below:

Figure 237: Enable method Lists Settings window



To delete an Enable Method List defined by the user, click the **Delete** button corresponding to the entry desired to be deleted. To modify an Enable Method List, click on its corresponding **Edit** button.

The fields that can be configured are described below:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *local_enable* - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The local enable password must be set by the user in the next section entitled Local Enable Password. *none* - Adding this parameter will require no authentication needed to access the Switch. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

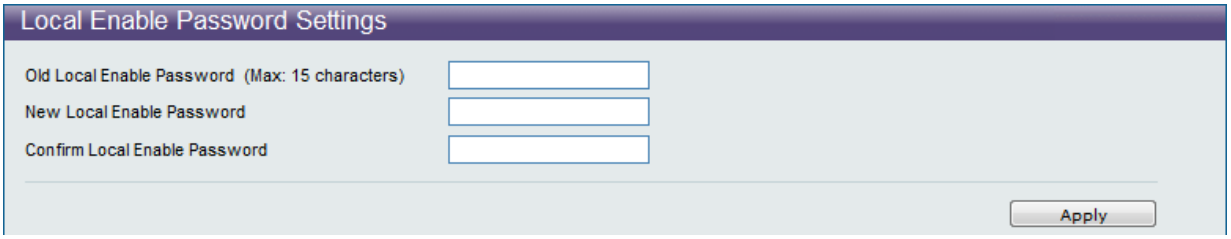
Click the **Delete** button to remove the specific entry.

Local Enable Password Settings

Users can configure the locally enabled password for Enable Admin. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view this window, click **Security > Access Authentication Control > Local Enable Password Settings** as shown below:

Figure 238: Local Enable Password Settings window


Local Enable Password Settings
Old Local Enable Password (Max: 15 characters)
New Local Enable Password
Confirm Local Enable Password
Apply

The fields that can be configured are described below:

Parameter	Description
Old Local Enable Password	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable Password	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Click the **Apply** button to accept the changes made.

SSL Settings

Secure Sockets Layer, or SSL, is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1 **Key Exchange:** The first part of the Cipher suite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.

2 **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

   Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

3 **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

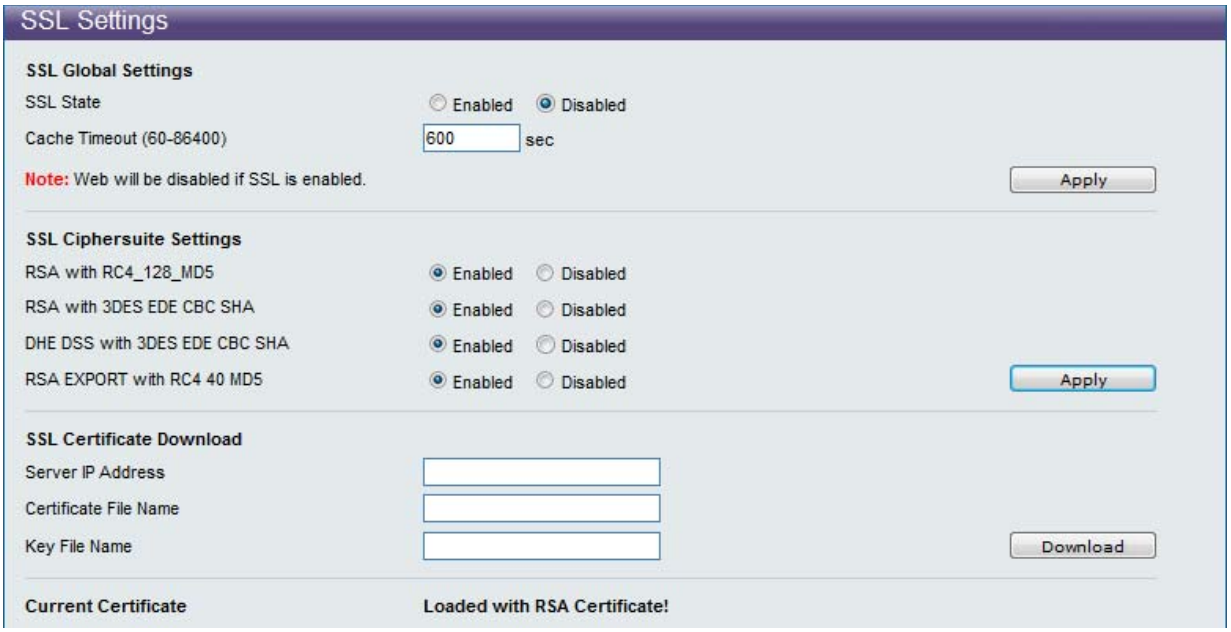
The SSL Settings window located on the next page will allow the user to enable SSL on the Switch and implement any one or combination of listed cipher suites on the Switch. A cipher suite is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible cipher suites for the SSL function, which are all enabled by default. To utilize a particular cipher suite, disable the unwanted cipher suites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

To view this window, click **Security > SSL Settings** as shown below:

Figure 239: SSL Settings window



To set up the SSL function on the Switch, configure the parameters in the SSL Settings section described.

The fields that can be configured are described below:

Parameter	Description
SSL Status	Use the radio buttons to enable or disable the SSL status on the Switch. The default is Disabled.
Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is *600* seconds.

Click the **Apply** button to accept the changes made.

To set up the **SSL cipher suite function** on the Switch, configure the parameters in the SSL Cipher suite Settings section described below:

Parameter	Description
RSA with RC4_128_MD5	This cipher suite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA with 3DES EDE CBC SHA	This cipher suite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.

Parameter	Description
DHS DSS with 3DES EDE CBC SHA	This cipher suite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA EXPORT with RC4 40 MD5	This cipher suite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.

Click the **Apply** button to accept the changes made.

To download SSL certificates, configure the parameters in the SSL Certificate Download section described below.

Parameter	Description
Server IP Address	Enter the IPv4 address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Nam	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

Click the **Download** button to download the SSL certificate based on the information entered.

NOTE

Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface.

NOTE

Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

SSH

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

1 Create a user account with admin-level access using the **User Accounts** window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This

password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.

2 Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication Mode** window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.

3 Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.

4 Finally, enable SSH on the Switch using the SSH Configuration window.

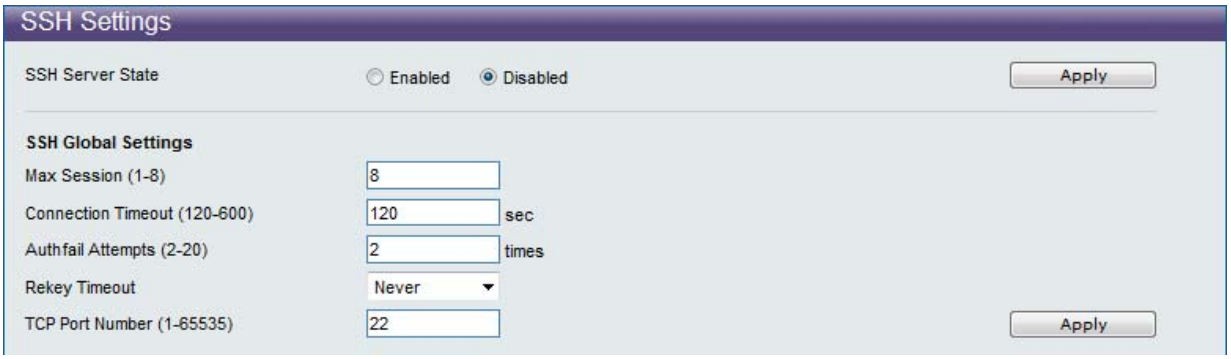
After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Settings

Users can configure and view settings for the SSH server.

To view this window, click **Security > SSH > SSH Settings** as shown below:

Figure 240: SSH Settings window



The fields that can be configured are described below:

Parameter	Description
SSH Server State	Use the radio buttons to enable or disable SSH on the Switch. The default is Disabled.
Max. Session	Enter a value between *1* and *8* to set the number of users that may simultaneously access the Switch. The default setting is *8*.
Connection Timeout	Allows the user to set the connection timeout. The user may set a time between *120* and *600* seconds. The default setting is *120* seconds.
Authfail Attempts	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.
Rekey Timeout	This field is used to set the time period that the Switch will change the security shell encryptions by using the pull-down menu. The available options are *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *Never*.

Parameter	Description
TCP Port Number	Here the user can enter the TCP Port Number used for SSH. The default value is *22*.

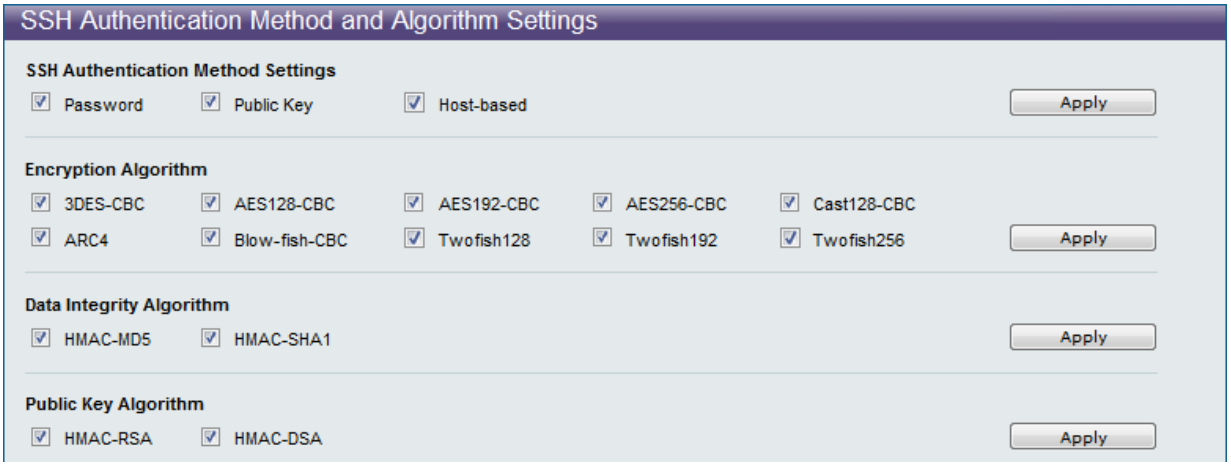
Click the **Apply** button to accept the changes made for each individual section.

SSH Authentication Method and Algorithm Settings

Users can configure the desired types of SSH algorithms used for authentication encryption. There are three categories of algorithms listed and specific algorithms of each may be enabled or disabled by ticking their corresponding check boxes. All algorithms are enabled by default.

To view this window, click **Security > SSH > SSH Authentication method and Algorithm Settings** as shown below:

Figure 241: SSH Authentication Method and Algorithm Settings window



The fields that can be configured for **SSH Authentication Mode** are described below:

Parameter	Description
Password	This may be enabled or disabled to choose if the administrator wishes to use a locally configured password for authentication on the Switch. This parameter is enabled by default.
Public Key	This may be enabled or disabled to choose if the administrator wishes to use a public key configuration set on a SSH server, for authentication. This parameter is enabled by default.
Host-based	This may be enabled or disabled to choose if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. This parameter is enabled by default.

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Encryption Algorithm** are described below:

Parameter	Description
3DES-CBC	Use the check box to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
Blow-fish CBC	Use the check box to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
AES128-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES192-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES256-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.
ARC4	Use the check box to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.
Cast128-CBC	Use the check box to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
Twofish128	Use the check box to enable or disable the twofish128 encryption algorithm. The default is enabled.
Twofish192	Use the check box to enable or disable the twofish192 encryption algorithm. The default is enabled.
Twofish256	Use the check box to enable or disable the twofish256 encryption algorithm. The default is enabled.

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Data Integrity Algorithm** are described below:

Parameter	Description
HMAC-SHA1	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.
HMAC-MD5	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Public Key Algorithm** are described below:

Parameter	Description
HMAC-RSA	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
HMAC-DSA	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm (DSA) encryption. The default is enabled.

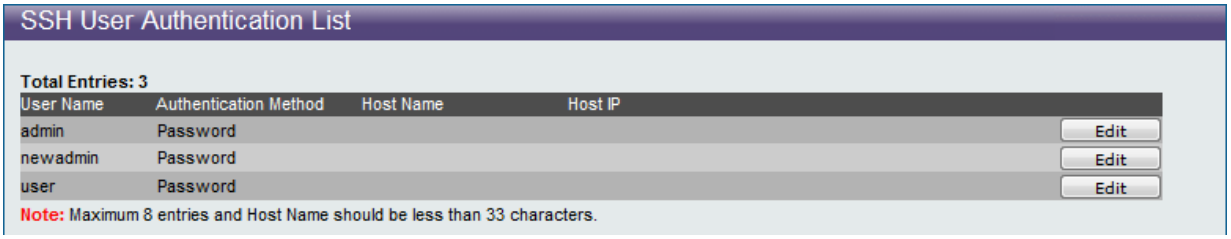
Click the **Apply** button to accept the changes made.

SSH User Authentication List

Users can configure parameters for users attempting to access the Switch through SSH. In the window above, the User Account "username" has been previously set using the **User Accounts** window in the **Configuration** folder. A User Account MUST be set in order to set the parameters for the SSH user.

To view this window, click **Security > SSH > SSH User Authentication List** as shown below:

Figure 242: SSH User Authentication List window



The fields that can be configured are described below:

Parameter	Description
User Name	A name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Authentication Method	The administrator may choose one of the following to set the authorization for users attempting to access the Switch. *Host Based* – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *Password* – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation. *Public Key* – This parameter should be chosen if the administrator wishes to use the public key on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Click the **Edit** button to re-configure the specific entry.

Click the **Apply** button to accept the changes made.

NOTE

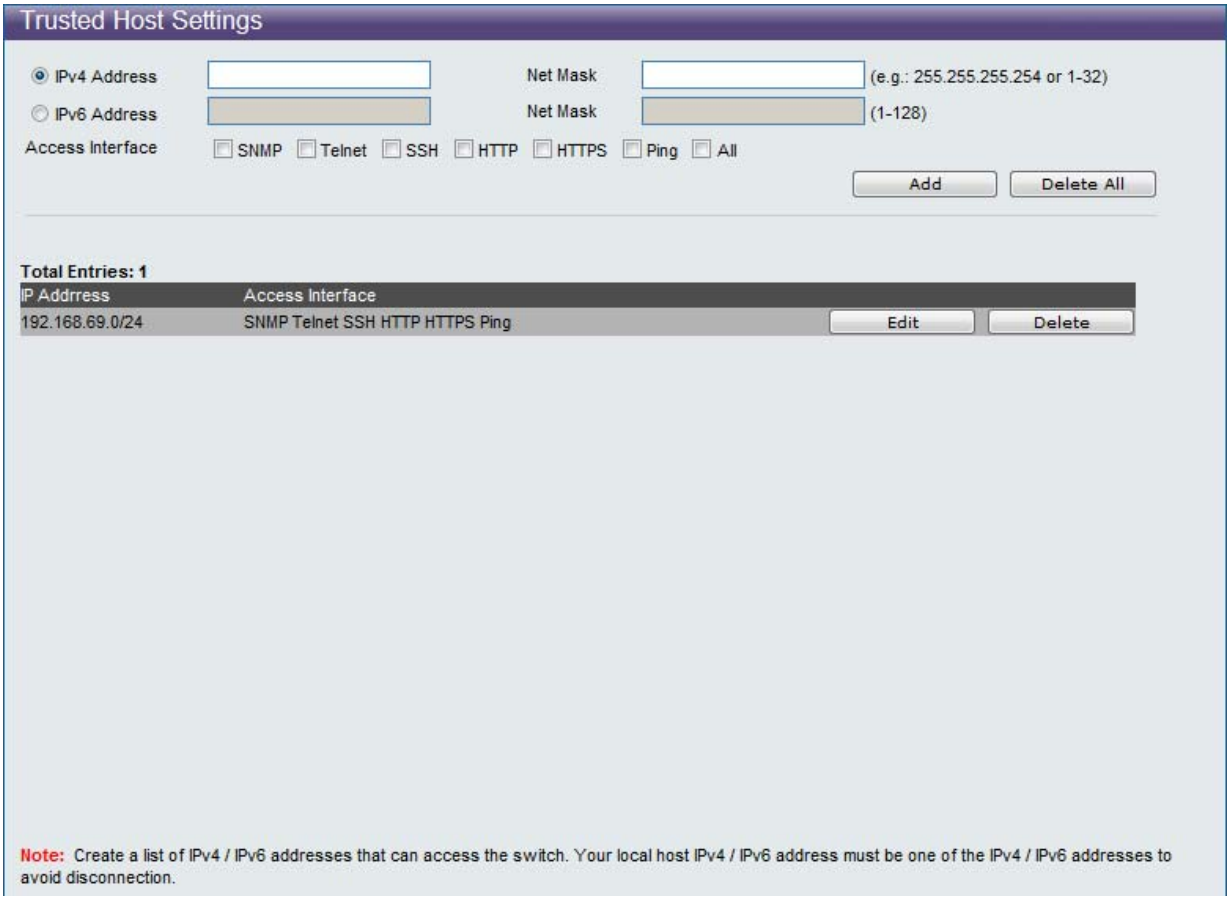
To set the SSH User Authentication Mode parameters on the Switch, a User Account must be previously configured.

Trusted Host Settings

Up to thirty trusted host secure IP addresses or ranges may be configured and used for remote Switch management. It should be noted that if one or more trusted hosts are enabled, the Switch will immediately accept remote instructions from only the specified IP address or addresses. If you enable this feature, be sure to first enter the IP address of the station you are currently using.

To view this window, click **Security > Trusted Host Settings** as shown below:

Figure 243: Trusted Host window



When the user clicks the **Edit** button, one will be able to edit the service allowed to the selected host.

The fields that can be configured are described below:

Parameter	Description
IPv4 Address	Enter an IPv4 address to add to the trusted host list.
IPv6 Address	Enter an IPv6 address to add to the trusted host list.
Net Mask	Enter a Net Mask address to add to the trusted host list.
Access Interface	Tick the check boxes to select services that will be allowed to the trusted host.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

9 Network Application

CHAPTER

DHCP

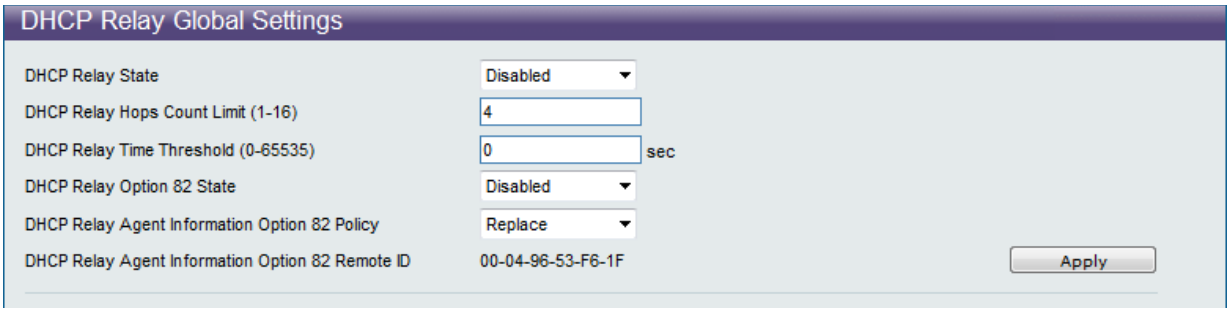
DHCP Relay

DHCP Relay Global Settings

Users can enable and configure DHCP Relay Global Settings. The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between *1* and *16* hops, with a default value of *4*. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds' field of the packet is less than the relay time threshold, the packet will be dropped. The range is between *0* and *65,535* seconds, with a default value of *0* seconds.

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Global Settings** as shown below:

Figure 244: DHCP Relay Global Settings window



The fields that can be configured are described below:

Parameter	Description
DHCP Relay State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Relay service on the Switch. The default is *Disabled.*

Parameter	Description
DHCP Relay Hops Count Limit (1-16)	This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP messages can be forwarded. The default hop count is *4*.
DHCP Relay Time Threshold (0-65535)	Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP packet. If a value of *0* is entered, the Switch will not process the value in the seconds' field of the DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given DHCP packet.
DHCP Relay Option 82 State	This field can be toggled between *Enabled* and *Disabled* using the pull-down menu. It is used to enable or disable the DHCP Relay Agent Information Option 82 on the Switch. The default is *Disabled*. *Enabled* –When this field is toggled to *Enabled*, the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *Disabled*- When the field is toggled to *Disabled*, the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Policy	This field can be toggled between *Replace, Drop,* and *Keep* by using the pull-down menu. It is used to set the Switches policy for handling packets when the DHCP Relay Agent Information Option 82 Check is set to *Disabled*. The default is *Replace.* *Replace* – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *Drop* – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *Keep* – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
DHCP Relay Agent Information Option 82 Remote ID	Here the user can view the DHCP Relay Agent Information Option 82 Remote ID.

Click the **Apply** button to accept the changes made for each individual section.

NOTE

If the Switch receives a packet that contains the option 82 field from a DHCP client and the information-checking feature is enabled, the Switch drops the packet because it is invalid. However, in some instances, users may configure a client with the option 82 field. In this situation, disable the information check feature so that the Switch does not remove the option 82 field from the packet. Users may configure the action that the Switch takes when it receives a packet with existing option 82 information by configuring the DHCP Agent Information Option 82 Policy.

The Implementation of DHCP Relay Agent Information Option 82

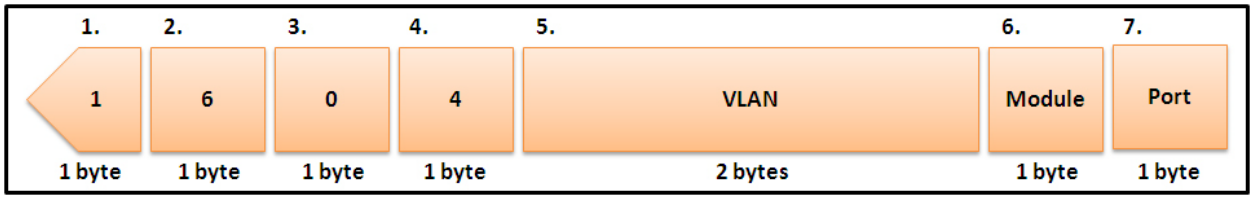
The **DHCP Relay Option 82** command configures the DHCP relay agent information option 82 setting of the Switch. The formats for the circuit ID sub-option and the remote ID sub-option are as follows:

NOTE

For the circuit ID sub-option of a standalone switch, the module field is always zero.

Circuit ID sub-option format:

Figure 245: Circuit ID Sub-option Format



1 Sub-option type

2 Length

3 Circuit ID type

4 Length

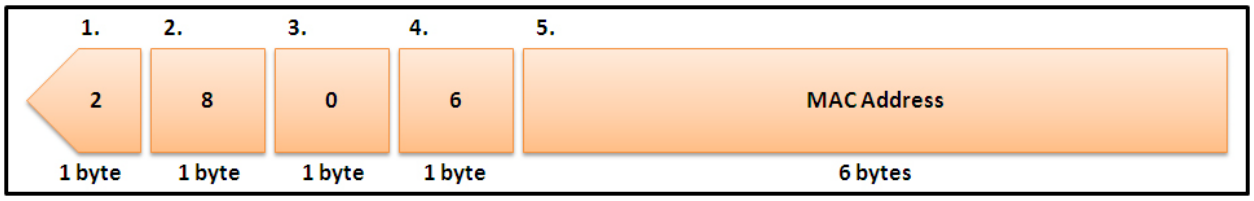
5 VLAN: The incoming VLAN ID of DHCP client packet.

6 Module: For a standalone switch, the Module is always 0; for a stackable switch, the Module is the Unit ID.

7 Port: The incoming port number of the DHCP client packet, the port number starts from 1.

Remote ID sub-option format:

Figure 246: Remote ID Sub-option Format



1 Sub-option type

2 Length

3 Remote ID type

4 Length

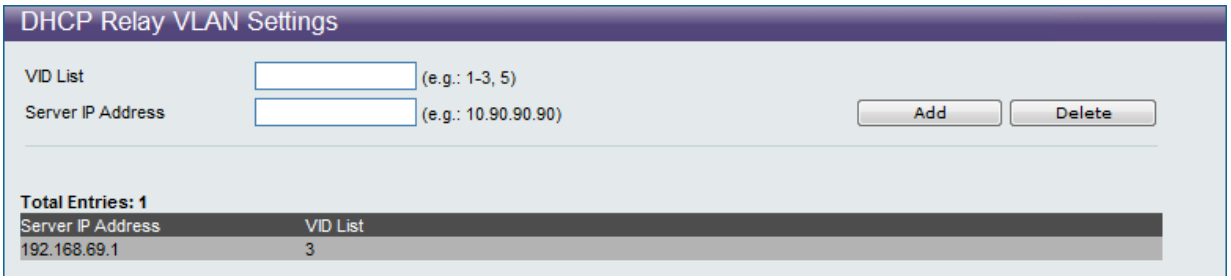
5 MAC address: The Switch's system MAC address.

DHCP Relay VLAN Settings

This page allows the user to configure an IP address as a destination to forward (relay) DHCP/BOOTP packets. If there is an IP interface in the VLAN and it has configured a DHCP server at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets.

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay VLAN Settings** as shown below:

Figure 247: DHCP Relay VLAN Settings window



The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used for this configuration here.
Server IP Address	Enter the DHCP/BOOTP server IP address used here.

Click the **Add** button to add an entry.

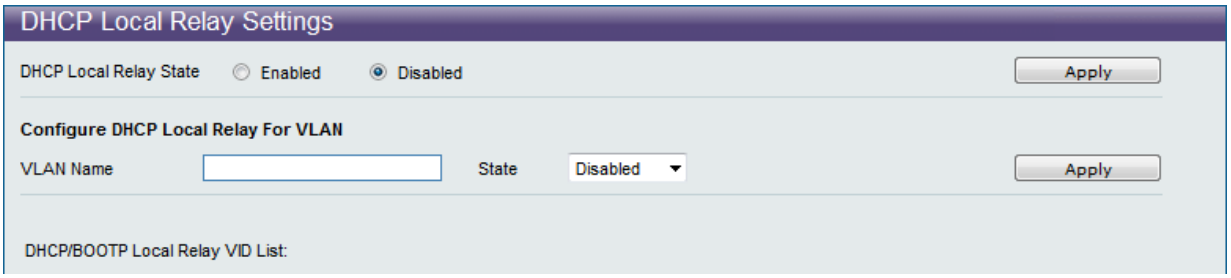
Click the **Delete** button to remove an entry.

DHCP Local Relay Settings

The DHCP local relay settings allows the user to add option 82 into DHCP request packets when the DHCP client gets an IP address from the same VLAN. If the DHCP local relay settings are not configured, the Switch will flood the packets to the VLAN. In order to add option 82 into the DHCP request packets, the DHCP local relay settings and the state of the Global VLAN need to be enabled.

To view this window, click **Network Application > DHCP > DHCP Local Relay Settings** as shown below:

Figure 248: DHCP Local Relay Settings window



The fields that can be configured are described below:

Parameter	Description
DHCP Local Relay Global State	Enable or disable the DHCP Local Relay Global State. The default is Disabled.
VLAN Name	This is the VLAN Name that identifies the VLAN the user wishes to apply the DHCP Local Relay operation.
State	Enable or disable the configure DHCP Local Relay for VLAN state.

Click the **Apply** button to accept the changes made for each individual section.

SNTP

The Simple Network Time Protocol (SNTP) is a protocol for synchronizing computer clocks through the Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the SNTP subnet of servers and clients, and adjust the system clock in each participant.

SNTP Settings

Users can configure the time settings for the Switch.

To view this window, click **Network Application > SNTP > SNTP Settings** as shown below:

Figure 249: SNTP Settings window

The fields that can be configured are described below:

Parameter	Description
SNTP State	Use this radio button to enable or disable SNTP.
Current Time	Displays the Current Time.
Time Source	Displays the time source for the system.
SNTP First Server	The IP address of the primary server from which the SNTP information will be taken.

Parameter	Description
SNTP Second Server	The IP address of the secondary server from which the SNTP information will be taken.
SNTP Poll Interval In Seconds (30-99999)	The interval, in seconds, between requests for updated SNTP information.

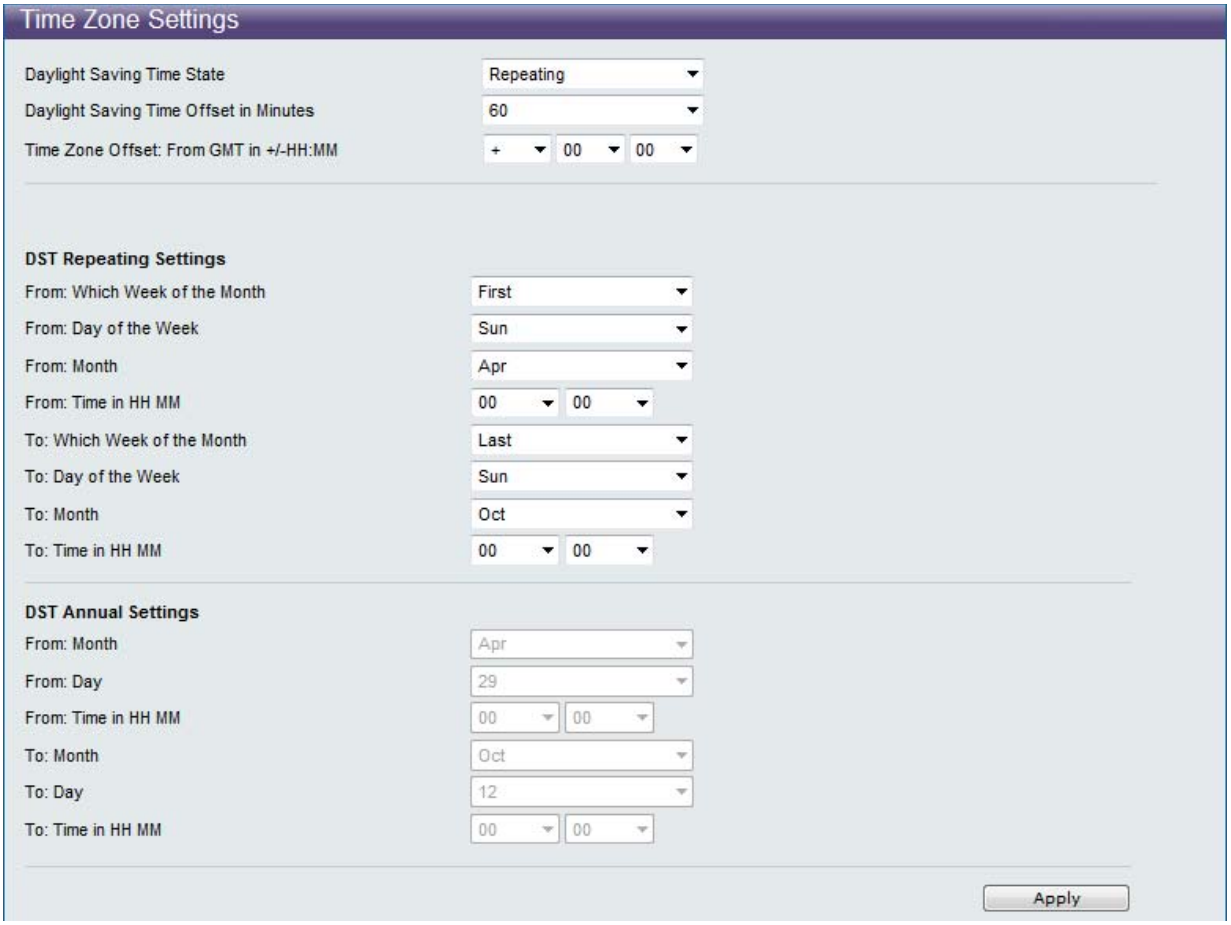
Click the **Apply** button to accept the changes made.

Time Zone Settings

Users can configure time zones and Daylight Savings Time settings for SNTP.

To view this window, click **Network Application > SNTP > Time Zone Settings** as shown below:

Figure 250: Time Zone Settings window



The fields that can be configured are described below:

Parameter	Description
Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.

Parameter	Description
Daylight Saving Time Offset In Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset – *30*, *60*, *90*, or *120* minutes.
Time Zone Offset From GMT In +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)

Parameter	Description
DST Repeating Settings	Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.
From: Which Week Of The Month	Enter the week of the month that DST will start.
From: Day Of Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: Time In HH:MM	Enter the time of day that DST will start on.
To: Which Week Of The Month	Enter the week of the month the DST will end.
To: Day Of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: Time In HH:MM	Enter the time DST will end.

Parameter	Description
DST Annual Settings	Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the month DST will start on, each year.
From: Time In HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the day of the month DST will end on, each year.
To: Time In HH:MM	Enter the time of day that DST will end on, each year.

Click the **Apply** button to accept the changes made.

Flash File System Settings

Why use flash file system:

In old switch system, the firmware, configuration and log information are saved in a flash with fixed addresses and size. This means that the maximum configuration file can only be 2Mb, and even if the current configuration is only 40Kb, it will still take up 2Mb of flash storage space. The configuration file number and firmware numbers are also fixed. A compatible issue will occur in the event that the configuration file or firmware size exceeds the originally designed size.

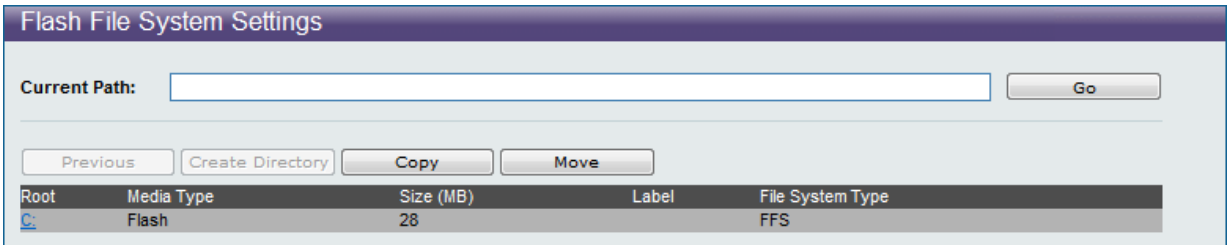
Flash File System in our system:

The Flash File System is used to provide the user with flexible file operation on the Flash. All the firmware, configuration information and system log information are stored in the Flash as files. This means that the Flash space taken up by all the files are not fixed, it is the real file size. If the Flash space is enough, the user could download more configuration files or firmware files and use commands to display Flash file information, rename file names, and delete it. Furthermore, the user can also configure the **boot up runtime image** or the **running configuration file** if needed.

In case the file system gets corrupted, Z-modem can be used to download the backup files directly to the system.

To view this window, click **Network Application > Flash File System Settings** as shown below:

Figure 251: Flash File System Settings window

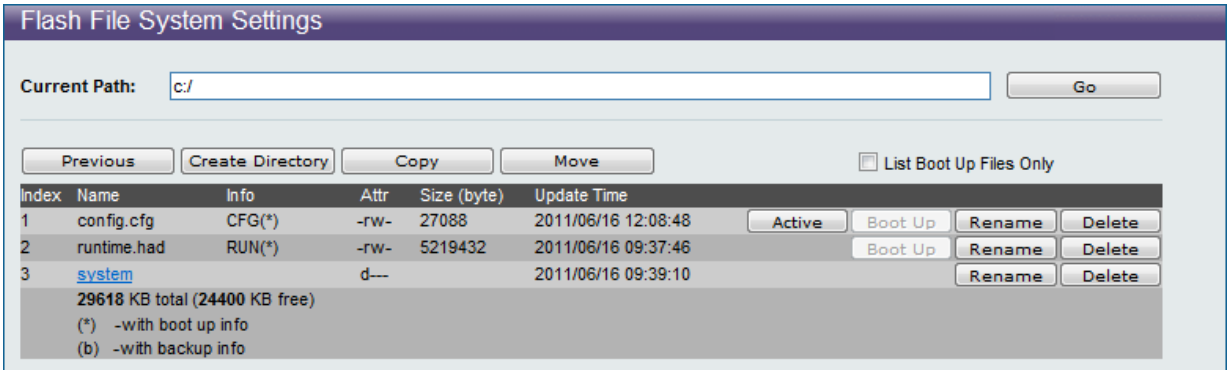


Enter the **Current Path** string and click the **Go** button to navigate to the path entered.

Click the **C:** link to navigate the C: drive

After clicking the **C:** link button, the following page will appear:

Figure 252: Flash File System Setting – Search for Drive window



Click the **Previous** button to return to the previous page.

Click the **Create Directory** to create a new directory within the file system of the switch.

Click the **Copy** button to copy a specific file to the switch.

Click the **Move** button to move a specific file within the switch.

Tick the **List Boot Up Files Only** option to display only the boot up files.

Click the Active button to set a specific config file as the active runtime configuration.

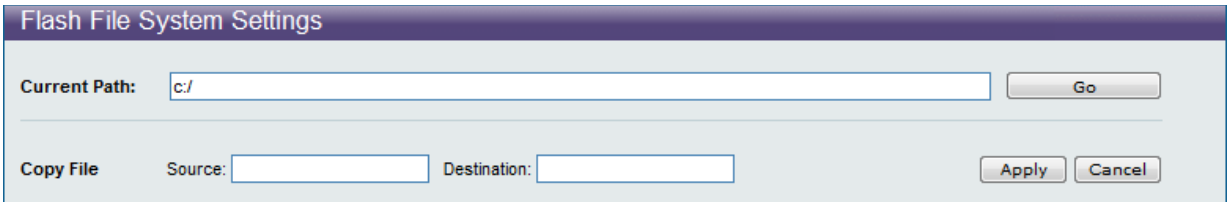
Click the **Boot Up** button to set a specific runtime image as the boot up image.

Click the **Rename** button to rename a specific file's name.

Click the **Delete** button to remove a specific file from the file system.

After clicking the **Copy** button, the following page will appear:

Figure 253: Flash File System Settings – Copy window



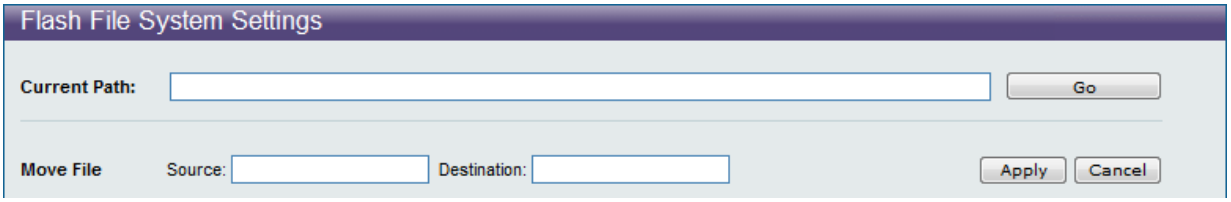
When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path.

Click the **Apply** button to initiate the copy.

Click the **Cancel** button the discard the process.

After clicking the **Move** button, the following page will appear:

Figure 254: Flash File System Settings – Move window



When moving a file to another place, the user must enter the **Source** and **Destination** path.

Click the **Apply** button to initiate the copy.

Click the **Cancel** button the discard the process.

10 CHAPTER OAM

CFM

CFM Settings

On this page the user can configure the CFM parameters.

To view this window, click **OAM > CFM > CFM Settings**, as shown below:

Figure 255: CFM Settings Window

The fields that can be configured are described below:

Parameter	Description
CFM State	Here the user can enable or disable the CFM feature.
All MPs Reply LTRs	Here the user can enable or disable all MPs to reply LTRs.
MD	Here the user can enter the maintenance domain name.
MD Index	Specifies the maintenance domain index used.
Level	Here the user can select the maintenance domain level.

Parameter	Description
MIP	This is the control creations of MIPs.
	None – Don't create MIPs. This is the default value.
	Auto – MIPs can always be created on any ports in this MD, if that port is not configured with a MEP of this MD. For the intermediate switch in a MA, the setting must be auto in order for the MIPs to be created on this device.
	Explicit – MIPs can be created on any ports in this MD, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MD.
SenderID TLV	This is the control transmission of the SenderID TLV.
	None – Don't transmit sender ID TLV. This is the default value.
	Chassis – Transmit sender ID TLV with chassis ID information.
	Manage – Transmit sender ID TLV with managed address information.
	Chassis Manage – Transmit sender ID TLV with chassis ID information and manage address information.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

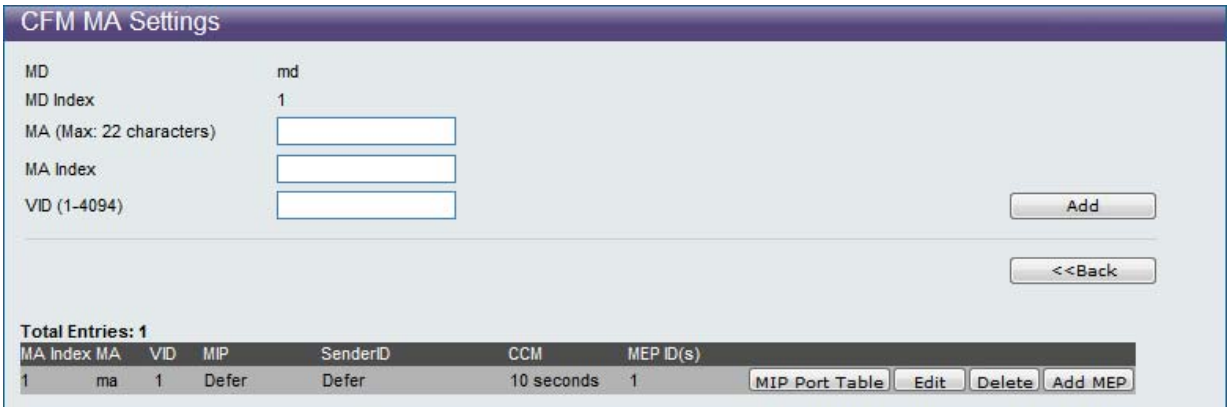
NOTE

The MD Name value should be less than 22 characters.

To add a maintenance association (MA), click on the **Add MA** button.

After clicking the **Add MA** button, the following page will appear:

Figure 256: CFM MA Settings Window



The fields that can be configured are described below:

Parameter	Description
MA	Here the user can enter the maintenance association name.
MA Index	Here the user can enter the maintenance association index.

Parameter	Description
VID	VLAN Identifier. Different MA must be associated with different VLANs.

Click the **Add** button to add a new entry based on the information entered.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Edit** button to re-configure the specific entry.

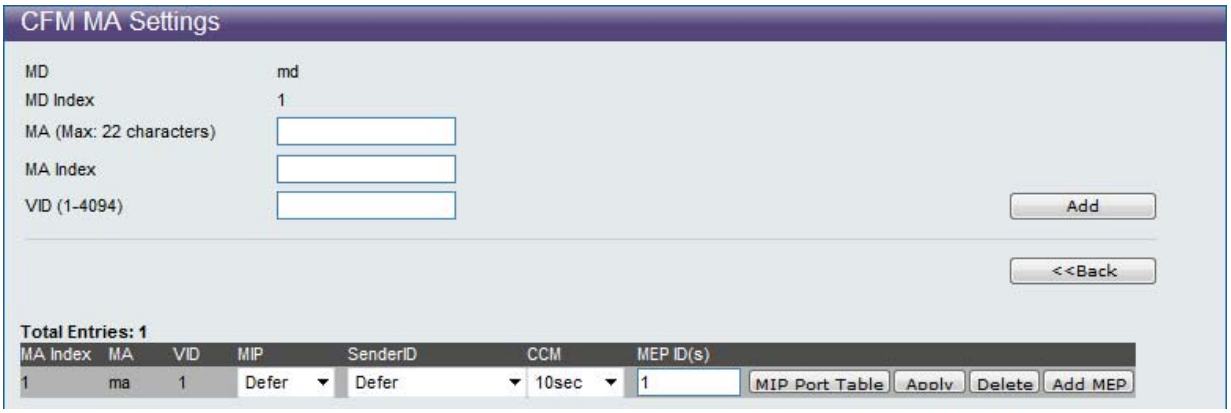
Click the **Delete** button to remove the specific entry.

Click the **MIP Port Table** button to view the CFM MIP Table.

Click the **Add MEP** button to add a Maintenance End Point entry.

After click in the **Edit** button the following window appears:

Figure 257: CFM MA Settings (Edit) Window



The fields that can be configured are described below:

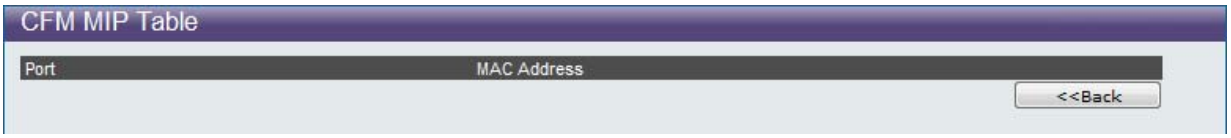
Parameter	Description
MIP	This is the control creation of MIPs. *None* - Don't create MIPs. *Auto* - MIPs can always be created on any ports in this MA, if that port is not configured with a MEP of that MA. *Explicit* - MIP can be created on any ports in this MA, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MA. *Defer* - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.

Parameter	Description
SenderID	This is the control transmission of the sender ID TLV.
	None - Don't transmit sender ID TLV. This is the default value.
	Chassis - Transmit sender ID TLV with chassis ID information.
	Manage - Transmit sender ID TLV with manage address information.
	Chassis Manage - Transmit sender ID TLV with chassis ID information and manage address information.
	Defer - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
CCM	This is the CCM interval.
	10ms - 10 milliseconds. Not recommended. For test purpose.
	100ms - 100 milliseconds. Not recommended. For test purpose.
	1sec - One second.
	10sec - Ten seconds. This is the default value.
	1min - One minute.
	10min - Ten minutes.
MEP ID(s)	This is to specify the MEP IDs contained in the maintenance association. The range of the MEP ID is 1-8191.
	Add - Add MEP ID(s).
	Delete - Delete MEP ID(s).
	By default, there is no MEP ID in a newly created maintenance association.

Click the **Apply** button to accept the changes made.

After clicking the **MIP Port Table** button, the following page will appear:

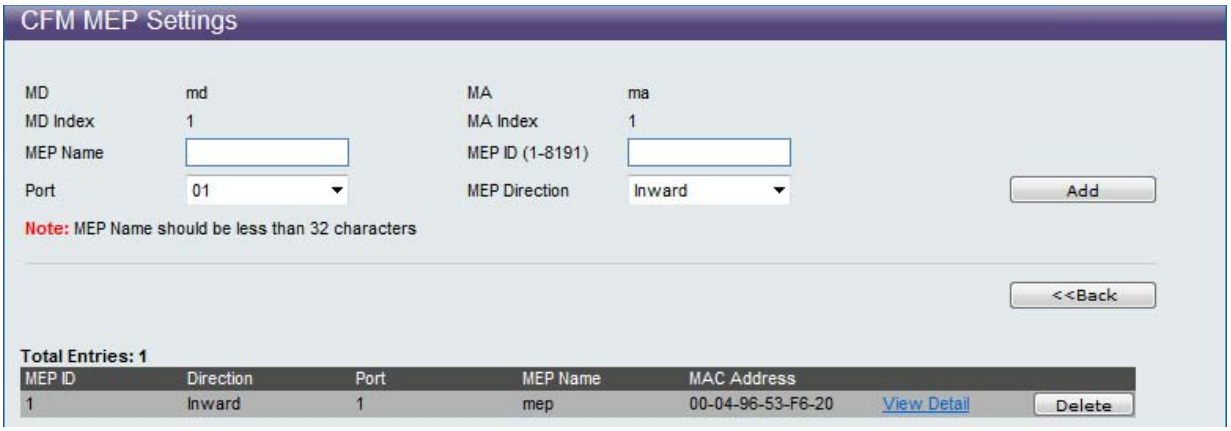
Figure 258: CFM MIP Port Table Window



Click the **<<Back** button to return to the previous page.

After clicking the **Add MEP** button, the following page will appear:

Figure 259: CFM MEP Settings (Add) Window



The fields that can be configured are described below:

Parameter	Description
MEP Name	MEP name. It is unique among all MEPs configured on the device.
MEP ID	MEP MEPID. It should be configured in the MA's MEP ID list.
Port	Port number. This port should be a member of the MA's associated VLAN.
MEP Direction	This is the MEP direction. *Inward* - Inward facing (up) MEP. *Outward* - Outward facing (down) MEP.

Click the **Add** button to add a new entry based on the information entered.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **View Detail** link to view more information regarding the specific entry.

Click the **Delete** button to remove the specific entry.

NOTE

The MEP Name value should be less than 32 characters.

After clicking the View Detail link, the following page will appear:

Figure 260: CFM MEP Information Window

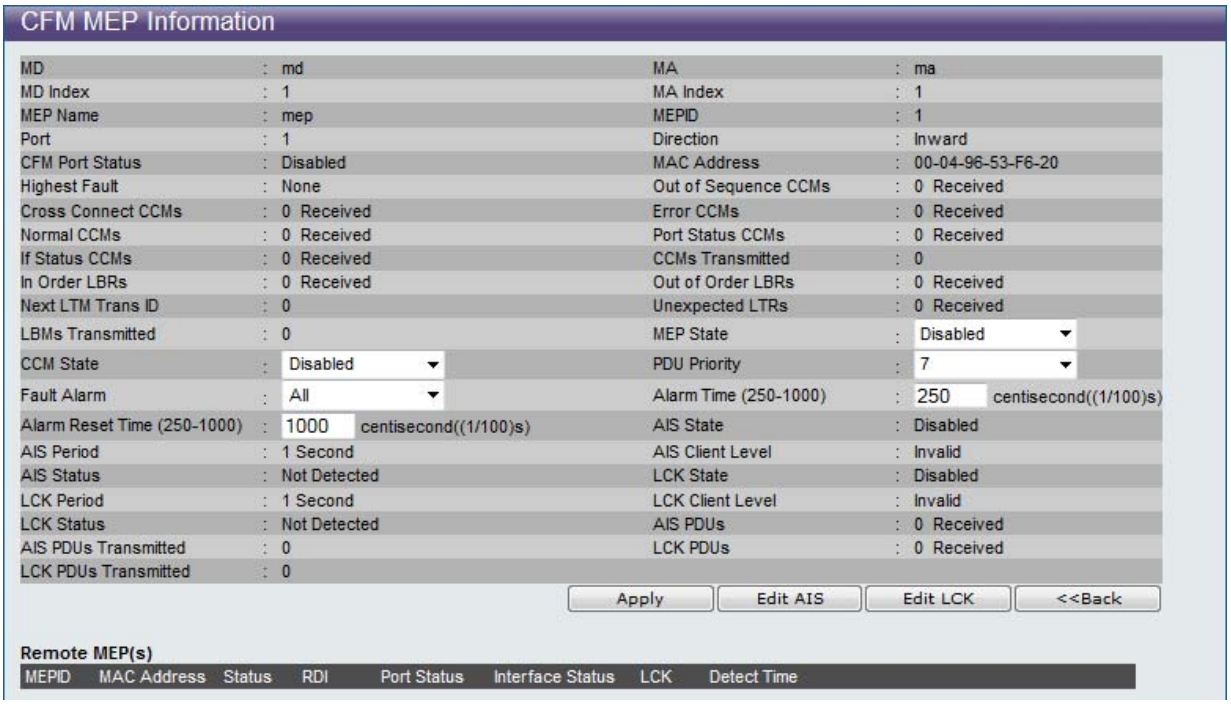
CFM MEP Information
MD : md
MD Index : 1
MEP Name : mep
Port : 1
CFM Port Status : Disabled
Highest Fault : None
Cross Connect CCMs : 0 Received
Normal CCMs : 0 Received
If Status CCMs : 0 Received
In Order LBRs : 0 Received
Next LTM Trans ID : 0
LBMs Transmitted : 0
CCM State : Disabled
Fault Alarm : Disabled
Alarm Reset Time (250-1000) : 1000 centisecond((1/100)s)
AIS Period : 1 Second
AIS Status : Not Detected
LCK Period : 1 Second
LCK Status : Not Detected
AIS PDUs Transmitted : 0
LCK PDUs Transmitted : 0
MA : ma
MA Index : 1
MEPID : 1
Direction : Inward
MAC Address : 00-04-96-53-F6-20
Out of Sequence CCMs : 0 Received
Error CCMs : 0 Received
Port Status CCMs : 0 Received
CCMs Transmitted : 0
Out of Order LBRs : 0 Received
Unexpected LTRs : 0 Received
MEP State : Disabled
PDU Priority : 7
Alarm Time (250-1000) : 250 centisecond((1/100)s)
AIS State : Disabled
AIS Client Level : Invalid
LCK State : Disabled
LCK Client Level : Invalid
AIS PDUs : 0 Received
LCK PDUs : 0 Received
Edit
Edit AIS
Edit LCK
<<Back
Remote MEP(s)
MEPID MAC Address Status RDI Port Status Interface Status LCK Detect Time

Click the **Edit** button to re-configure the specific entry.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Edit** button, the following page will appear:

Figure 261: CFM MEP Information (Edit) Window


CFM MEP Information
MD : md
MD Index : 1
MEP Name : mep
Port : 1
CFM Port Status : Disabled
Highest Fault : None
Cross Connect CCMs : 0 Received
Normal CCMs : 0 Received
If Status CCMs : 0 Received
In Order LBRs : 0 Received
Next LTM Trans ID : 0
LBMs Transmitted : 0
CCM State : Disabled
Fault Alarm : All
Alarm Reset Time (250-1000) : 1000 centisecond((1/100)s)
AIS Period : 1 Second
AIS Status : Not Detected
LCK Period : 1 Second
LCK Status : Not Detected
AIS PDUs Transmitted : 0
LCK PDUs Transmitted : 0
MA : ma
MA Index : 1
MEPID : 1
Direction : Inward
MAC Address : 00-04-96-53-F6-20
Out of Sequence CCMs : 0 Received
Error CCMs : 0 Received
Port Status CCMs : 0 Received
CCMs Transmitted : 0
Out of Order LBRs : 0 Received
Unexpected LTRs : 0 Received
MEP State : Disabled
PDU Priority : 7
Alarm Time (250-1000) : 250 centisecond((1/100)s)
AIS State : Disabled
AIS Client Level : Invalid
LCK State : Disabled
LCK Client Level : Invalid
AIS PDUs : 0 Received
LCK PDUs : 0 Received
Apply
Edit AIS
Edit LCK
<<Back
Remote MEP(s)
MEPID MAC Address Status RDI Port Status Interface Status LCK Detect Time

The fields that can be configured are described below:

Parameter	Description
MEP State	This is the MEP administrative state. *Enable* - MEP is enabled. *Disable* - MEP is disabled. This is the default value.
CCM State	This is the CCM transmission state. *Enable* - CCM transmission enabled. *Disable* - CCM transmission disabled. This is the default value.
PDU Priority	The 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7.
Fault Alarm	This is the control types of the fault alarms sent by the MEP. *All* - All types of fault alarms will be sent. *MAC Status* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Error” are sent. *Remote CCM* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP Down” are sent. *Errors CCM* - Only the fault alarms whose priority is equal to or higher than “Error CCM Received” are sent. *Xcon CCM* - Only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” are sent. *None* - No fault alarm is sent. This is the default value.
Alarm Time	This is the time that a defect must exceed before the fault alarm can be sent. The unit is in centiseconds, the range is 250-1000. The default value is 250.

Parameter	Description
Alarm Reset Time	This is the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is in centiseconds, the range is 250-1000. The default value is 1000

Click the **Apply** button to accept the changes made.

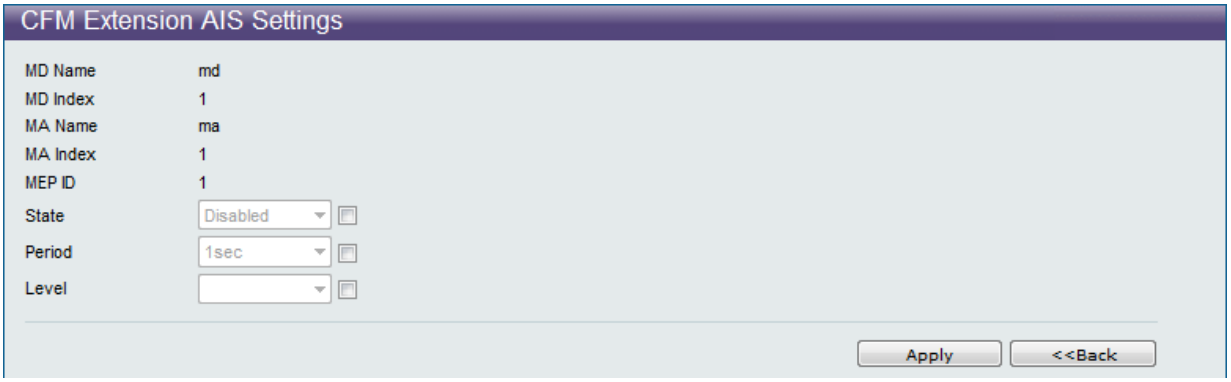
Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Edit AIS** button to configure the AIS settings.

Click the **Edit LCK** button to configure the LCK settings.

After clicking the **Edit AIS** button, the following window will appear:

Figure 262: CFM Extension AIS (Edit) Window



The fields that can be configured are described below:

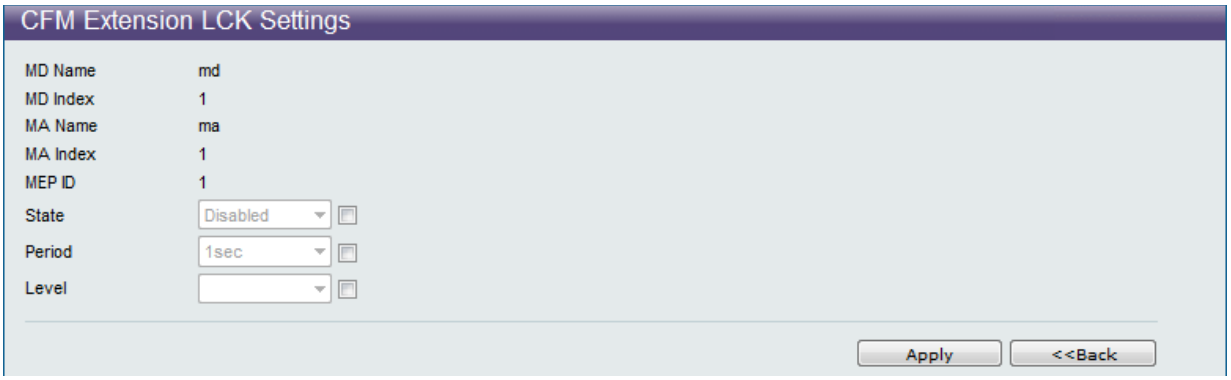
Parameter	Description
State	Specifies to *enable* or *disable* the AIS function.
Period	The transmitting interval of AIS PDU. The default period is 1 second. Options to choose from are: *1sec* - Specifies that the transmitting interval will be set to 1 second. *1min* - Specifies that the transmitting interval will be set to 1 minute.
Level	The client level ID to which the MEP sends AIS PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between *0-7*.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After click the **Edit LCK** button, the following window will appear:

Figure 263: CFM Extension LCK Settings (Edit) Window



The fields that can be configured are described below:

Parameter	Description
State	Specifies to *enable* or *disable* the LCK function.
Period	The transmitting interval of LCK PDU. The default period is 1 second. Options to choose from are: *1sec* - Specifies that the transmitting interval will be set to 1 second. *1min* - Specifies that the transmitting interval will be set to 1 minute.
Level	The client level ID to which the MEP sends LCK PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between *0-7*.

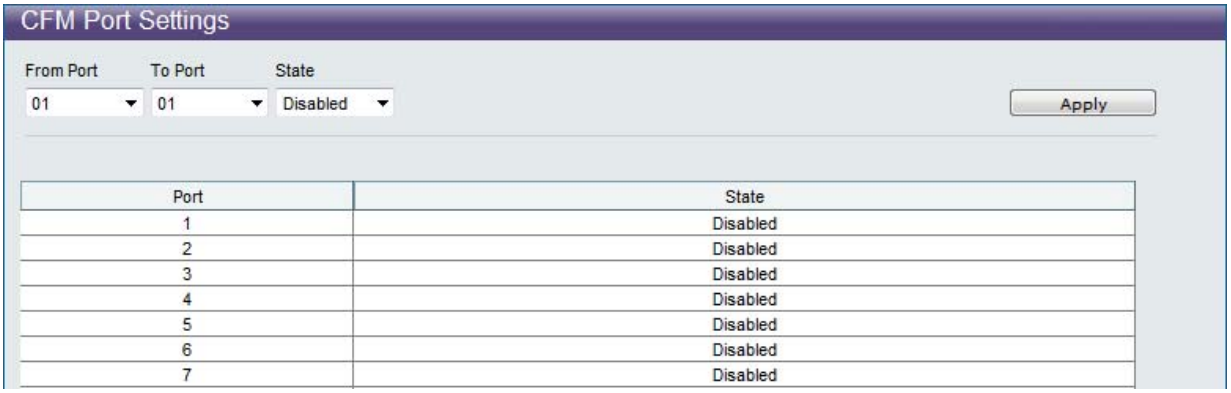
Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

CFM Port Settings

To view this window, click **OAM > CFM > CFM Port Settings**, as shown below:

Figure 264: CFM Port Settings Window



The fields that can be configured are described below:

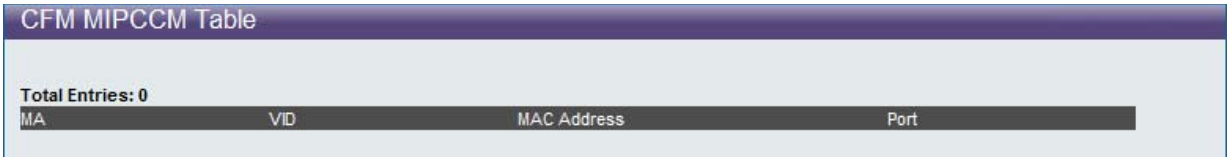
Parameter	Description
From Port ~ To Port	Here the user can select the port range used for this configuration.
State	Here the user can enable or disable the state of specific port regarding the CFM configuration.

Click the **Apply** button to accept the changes made.

CFM MIPCCM Table

To view this window, click **OAM > CFM > CFM MIPCCM Table**, as shown below:

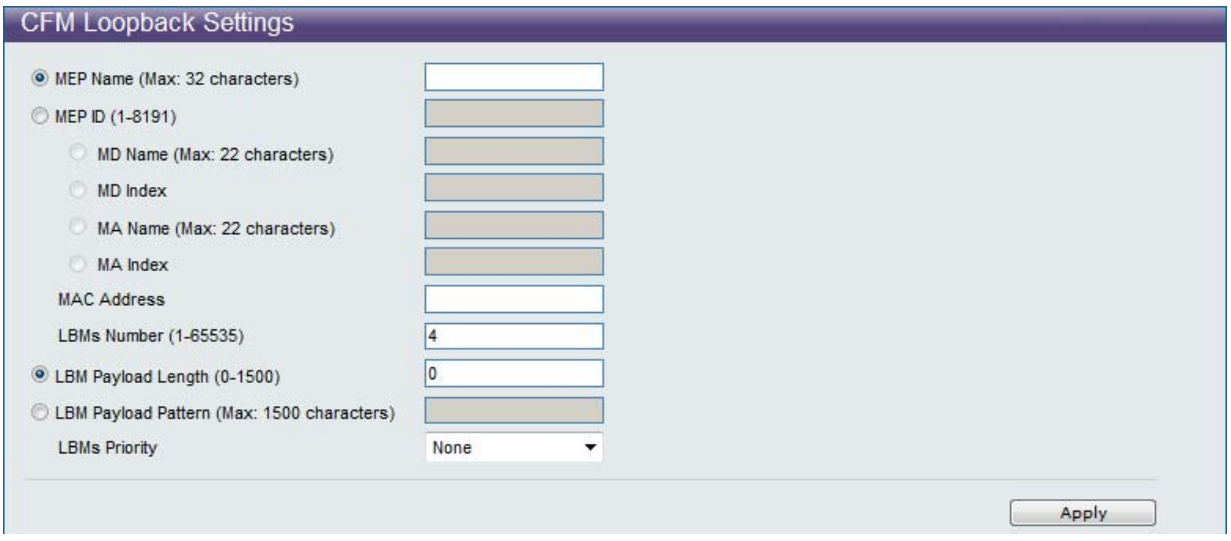
Figure 265: CFM MIPCCM Table Window



CFM Loopback Settings

To view this window, click **OAM > CFM > CFM Loopback Settings**, as shown below:

Figure 266: CFM Loopback Settings Window



The fields that can be configured are described below:

Parameter	Description
MEP Name	Select and enter the Maintenance End Point name used.
MEP ID	Select and enter the Maintenance End Point ID used.
MD Name	Select and enter the Maintenance Domain name used.

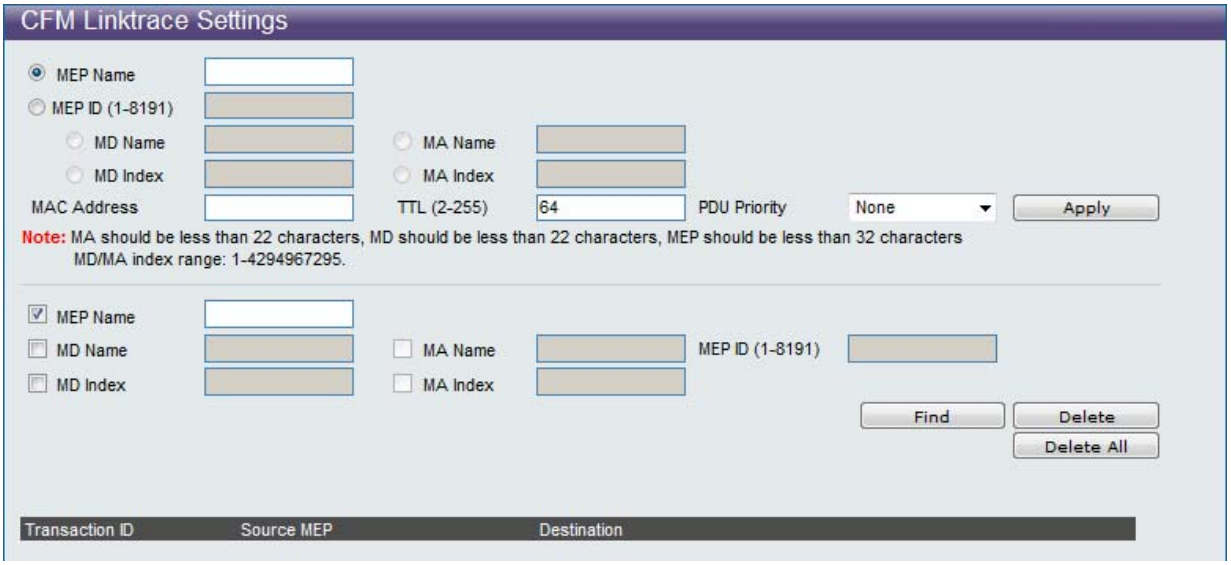
Parameter	Description
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.
MAC Address	Enter the destination MAC address used here.
LBMs Number	Number of LBMs to be sent. The default value is 4.
LBM Payload Length	The payload length of LBM to be sent. The default is 0.
LBM Payload Pattern	An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included.
LBMs Priority	The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA.

Click the **Apply** button to accept the changes made.

CFM Linktrace Settings

To view this window, click **OAM > CFM > CFM Linktrace Settings**, as shown below:

Figure 267: CFM Linktrace Settings Window



The fields that can be configured are described below:

Parameter	Description
MEP Name	Select and enter the Maintenance End Point name used.
MEP ID	Select and enter the Maintenance End Point ID used.
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.

Parameter	Description
MAC Address	Here the user can enter the destination MAC address.
TTL	Link-trace message TTL value. The default value is 64.
PDU Priority	The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

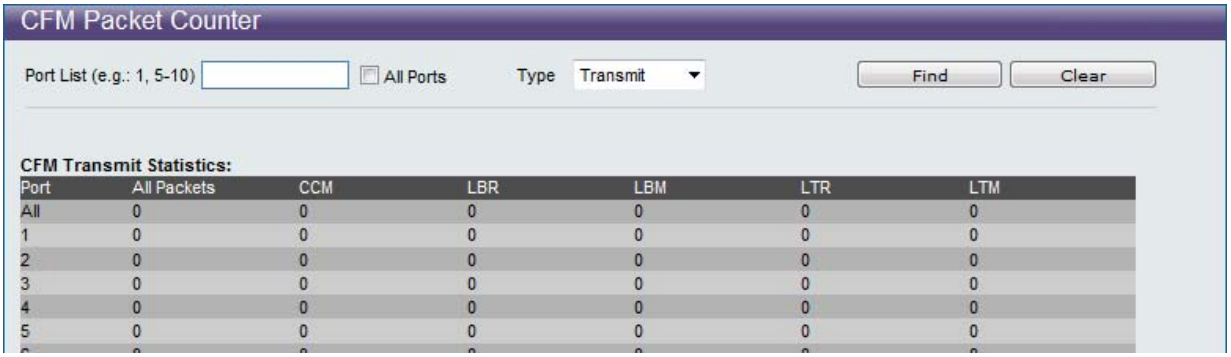
Click the **Delete** button to remove the specific entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

CFM Packet Counter

To view this window, click **OAM > CFM > CFM Packet Counter**, as shown below:

Figure 268: CFM Packet Counter Window



The fields that can be configured are described below:

Parameter	Description
Port List	Which ports' counter to show. If not specified, all ports will be shown.
All Ports	Select this option to include all the port in this configuration.
Type	*Transmit* – Selecting this option will display all the CFM packets transmitted. *Receive* – Selecting this option will display all the CFM packets received. *CCM* – Selecting this option will display all the CFM packets transmitted and received.

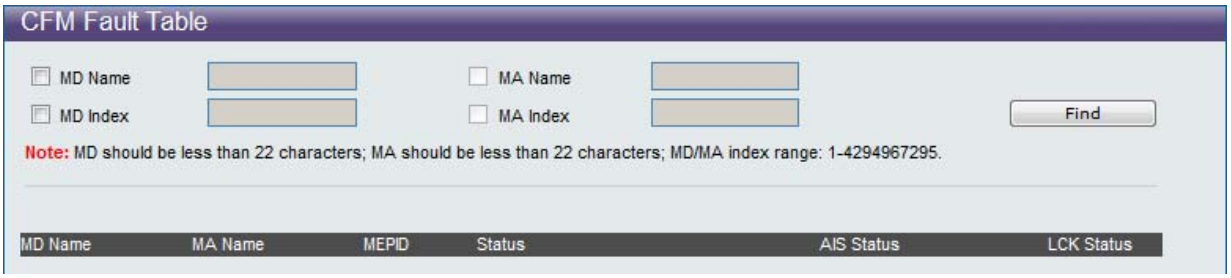
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information entered in the fields.

CFM Fault Table

To view this window, click **OAM > CFM > CFM Fault Table**, as shown below:

Figure 269: CFM Fault Table Window



The fields that can be configured are described below:

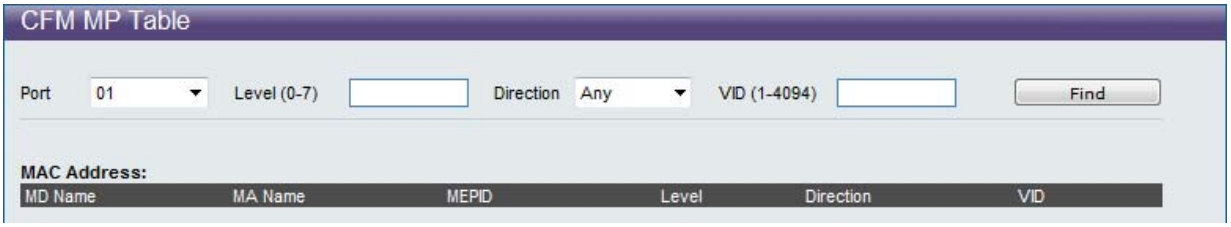
Parameter	Description
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.

Click the **Find** button to locate a specific entry based on the information entered.

CFM MP Table

To view this window, click **OAM > CFM > CFM MP Table**, as shown below:

Figure 270: CFM MP Table Window



The fields that can be configured are described below:

Parameter	Description
Port	Here the user can select the port number to view.
Level	Here the user can enter the level to view.
Direction	Here the user can enter the direction to view.
	Inward - Inward facing (up) MP.
	Outward - Outward facing (down) MP.
VID	Here the user can enter the VID to view.

Click the **Find** button to locate a specific entry based on the information entered.

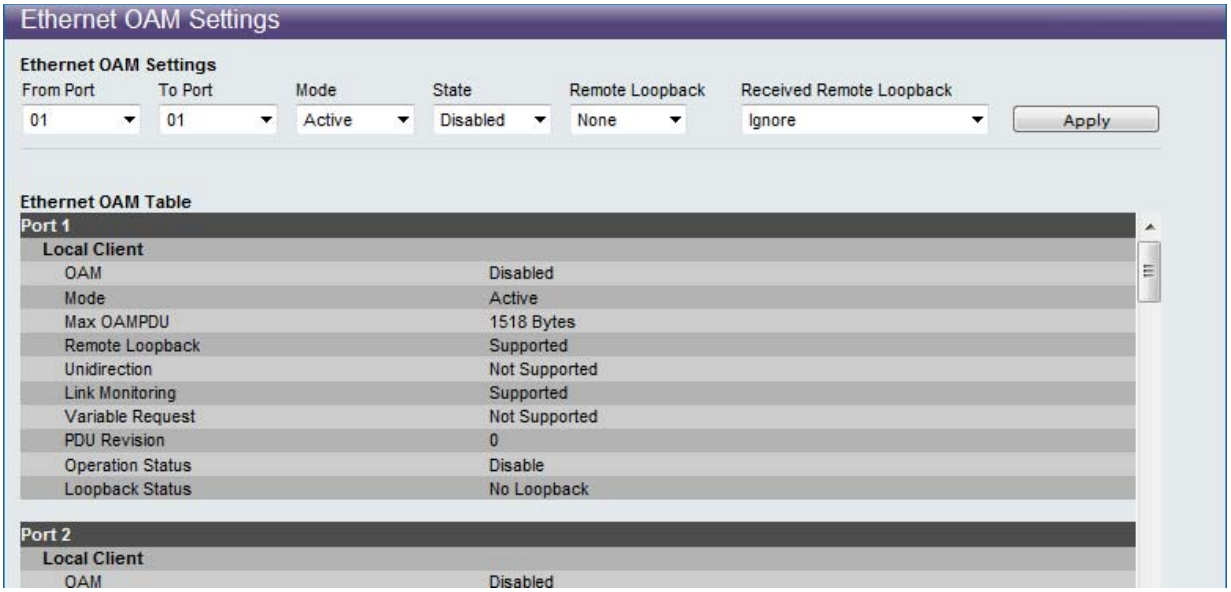
Ethernet OAM

Ethernet OAM Settings

This window is used to configure the Ethernet OAM settings.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Settings**, as shown below:

Figure 271: Ethernet OAM Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports you wish to configure.
Mode	Use the drop-down menu to select to operate in either *Active* or *Passive*. The default mode is Active.
State	Use the drop-down menu to enable or disable the OAM function.
Remote Loopback	Use the drop-down menu to select Ethernet OAM remote loopback. *None* – Select to disable the remote loopback. *Start* – Select to request the peer to change to the remote loopback mode. *Stop* Select to request the peer to change to the normal operation mode.
Received Remote Loopback	Use the drop-down menu to configure the client to process or to ignore the received Ethernet OAM remote loopback command. *Process* – Select to process the received Ethernet OAM remote loopback command. *Ignore* Select to ignore the received Ethernet OAM remote loopback command.

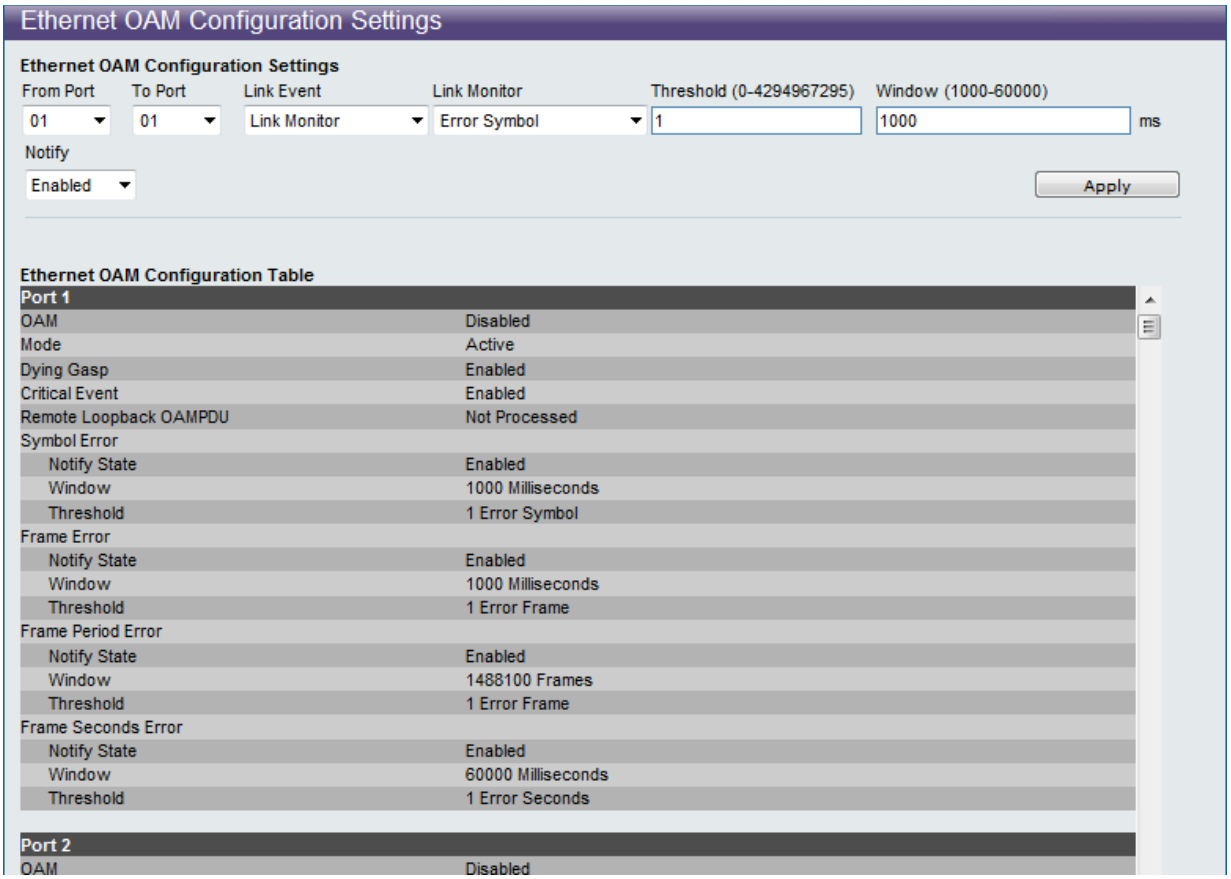
Click the **Apply** button to accept the changes made for each individual section.

Ethernet OAM Configuration Settings

This window is used to configure Ethernet OAM configuration settings.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Configuration Settings**, as shown below:

Figure 272: Ethernet OAM Configuration Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select a range of ports you wish to configure.
Link Event	Use the drop-down menu to select the link events, *Link Monitor* or *Critical Link Event*.
Link Monitor	Use the drop-down menu to select link monitor. Available options are *Error Symbol*, *Error Frame*, *Error Frame Period*, and *Error Frame Seconds*.
Critical Link Event	Use the drop-down menu to select between *Dying Gasp* and *Critical Event*.
Threshold	Enter the number of error frame or symbol in the period is required to be equal to or greater than in order for the event to be generated.
Window	Enter the period of error frame or symbol in milliseconds summary event.

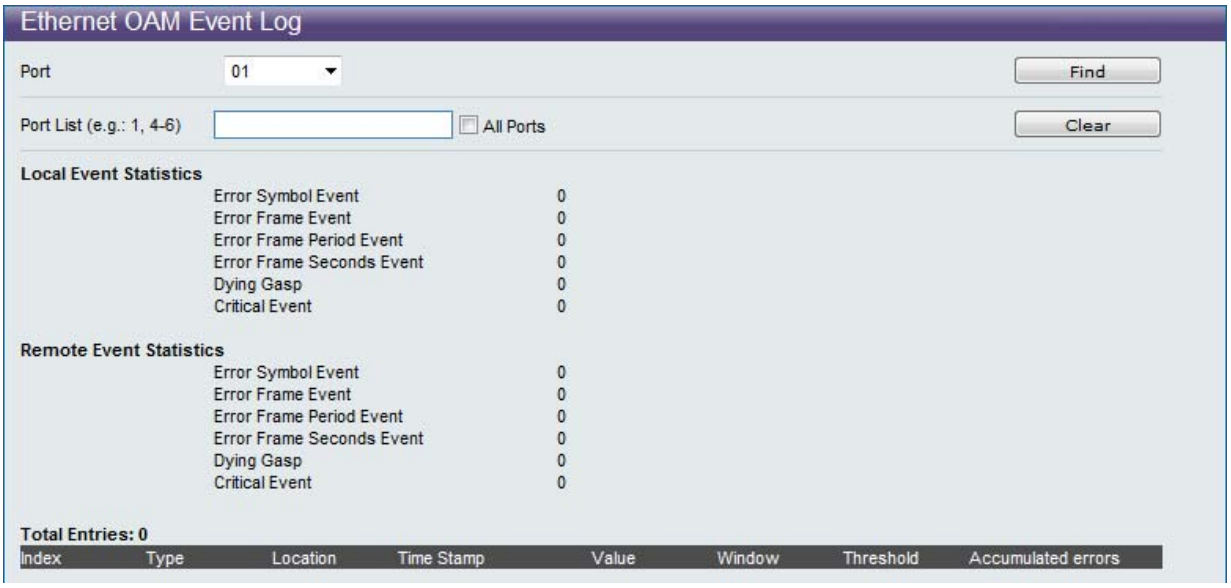
Click the **Apply** button to accept the changes made for each individual section.

Ethernet OAM Event Log

The window is used to show ports Ethernet OAM event log information.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Event Log**, as shown below:

Figure 273: Ethernet OAM Event Log window



The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select the port number to view.
Port List	Enter a list of ports. Tick the **All Ports** check box to select all ports.

Click the **Find** button to locate a specific entry based on the information entered.

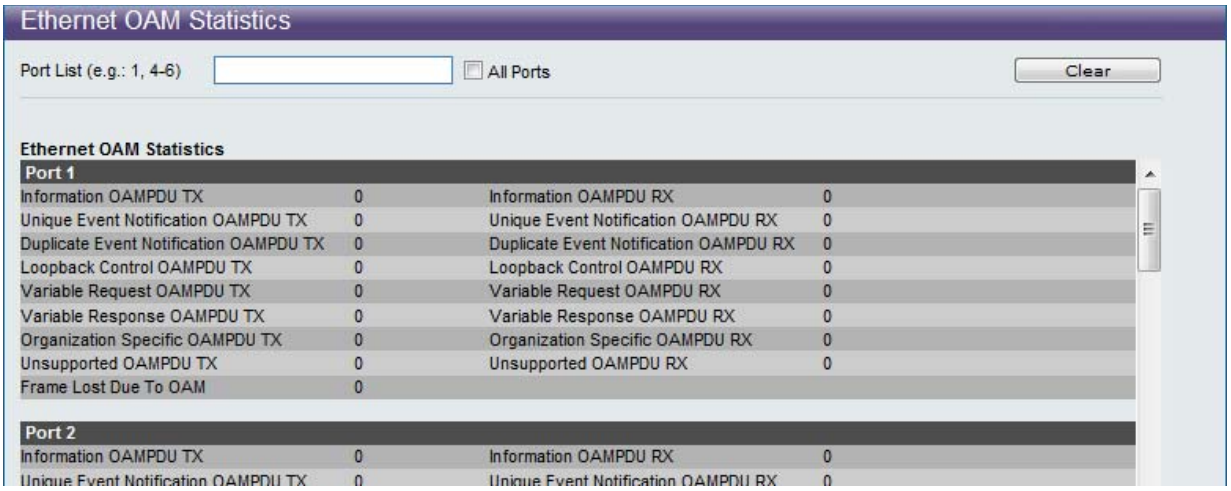
Click the **Clear** button to clear all the information entered in the fields.

Ethernet OAM Statistics

The window is used to show ports Ethernet OAM statistics information.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Statistics**, as shown below:

Figure 274: Ethernet OAM Statistics window


Ethernet OAM Statistics
Port List (e.g.: 1, 4-6)
All Ports
Clear
Ethernet OAM Statistics
Port 1
Information OAMPDU TX 0
Information OAMPDU RX 0
Unique Event Notification OAMPDU TX 0
Unique Event Notification OAMPDU RX 0
Duplicate Event Notification OAMPDU TX 0
Duplicate Event Notification OAMPDU RX 0
Loopback Control OAMPDU TX 0
Loopback Control OAMPDU RX 0
Variable Request OAMPDU TX 0
Variable Request OAMPDU RX 0
Variable Response OAMPDU TX 0
Variable Response OAMPDU RX 0
Organization Specific OAMPDU TX 0
Organization Specific OAMPDU RX 0
Unsupported OAMPDU TX 0
Unsupported OAMPDU RX 0
Frame Lost Due To OAM 0
Port 2
Information OAMPDU TX 0
Information OAMPDU RX 0

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select the port number to view.
Port List	Enter a list of ports. Tick the **All Ports** check box to select all ports.

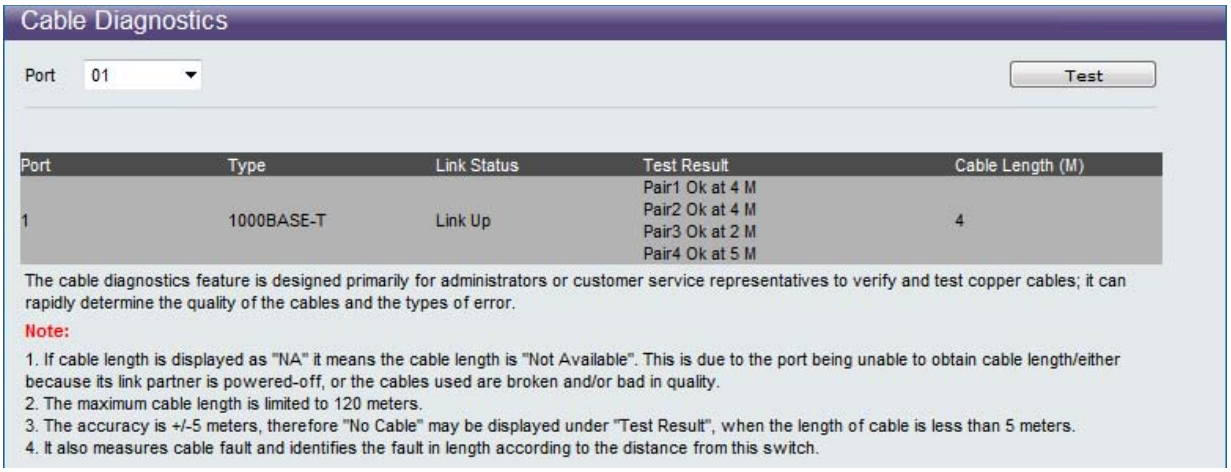
Click the **Clear** button to clear all the information entered in the fields.

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view this window, click **OAM > Cable Diagnostics** as shown below:

Figure 275: Cable Diagnostics window


Cable Diagnostics
Port
01
Test
Port
Type
Link Status
Test Result
Cable Length (M)
1
1000BASE-T
Link Up
Pair1 Ok at 4 M
Pair2 Ok at 4 M
Pair3 Ok at 2 M
Pair4 Ok at 5 M
4
The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.
Note:
1. If cable length is displayed as "NA" it means the cable length is "Not Available". This is due to the port being unable to obtain cable length/either because its link partner is powered-off, or the cables used are broken and/or bad in quality.
2. The maximum cable length is limited to 120 meters.
3. The accuracy is +/-5 meters, therefore "No Cable" may be displayed under "Test Result", when the length of cable is less than 5 meters.
4. It also measures cable fault and identifies the fault in length according to the distance from this switch.

To view the cable diagnostics for a particular port, use the drop-down menu to choose the port and click **Test** The information will be displayed in this window.

NOTE

Cable diagnostic function limitations. Cable length detection is only supported on GE ports. Ports must be linked up and running at 1000M speed. Cross-talk errors detection is not supported on FE ports.

NOTE

The available cable diagnosis length is from 5 to 120 meters.

NOTE

The deviation of cable length detection is +/- 5M for GE ports.

Fault messages:

- *Open* - This pair is left open.
- *Short* - Two lines of this pair is shorted.
- *CrossTalk* - Lines of this pair is short with lines in other pairs.
- *Unknown* - The diagnosis does not obtain the cable status, please try again.
- *NA* - No cable was found, maybe it's because cable is out of diagnosis specification or the quality is too bad.

11 Monitoring

CHAPTER

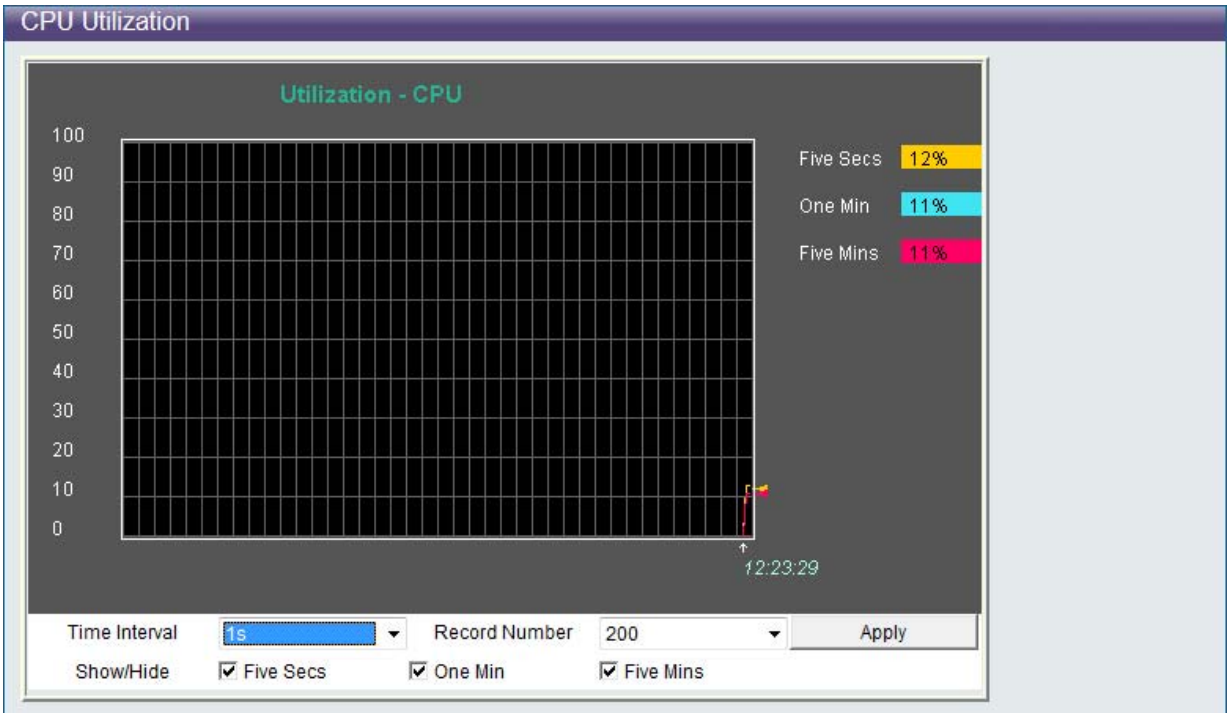
Utilization

CPU Utilization

Users can display the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.

To view this window, click **Monitoring > Utilization > CPU Utilization** as shown below:

Figure 276: CPU Utilization window



To view the CPU utilization by port, use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

The fields that can be configured are described below:

Parameter	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Five Seconds, One Minute, and Five Minutes.

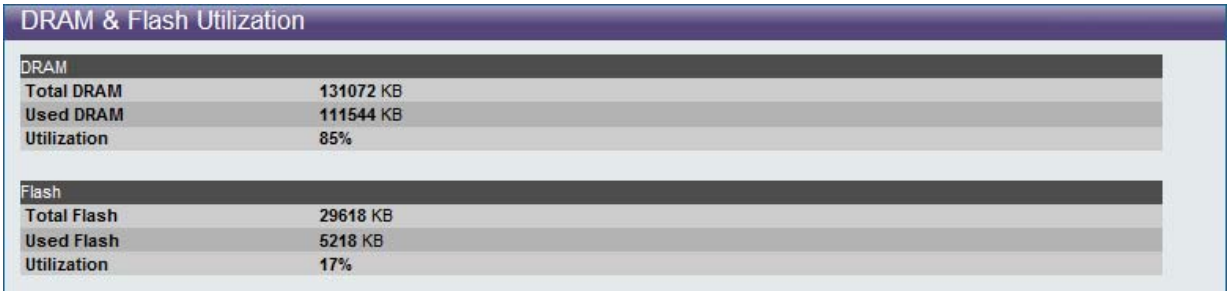
Click the **Apply** button to accept the changes made.

DRAM & Flash Utilization

On this page the user can view information regarding the DRAM and Flash utilization.

To view this window, click **Monitoring > Utilization > DRAM & Flash Utilization** as shown below:

Figure 277: DRAM & Flash Utilization window

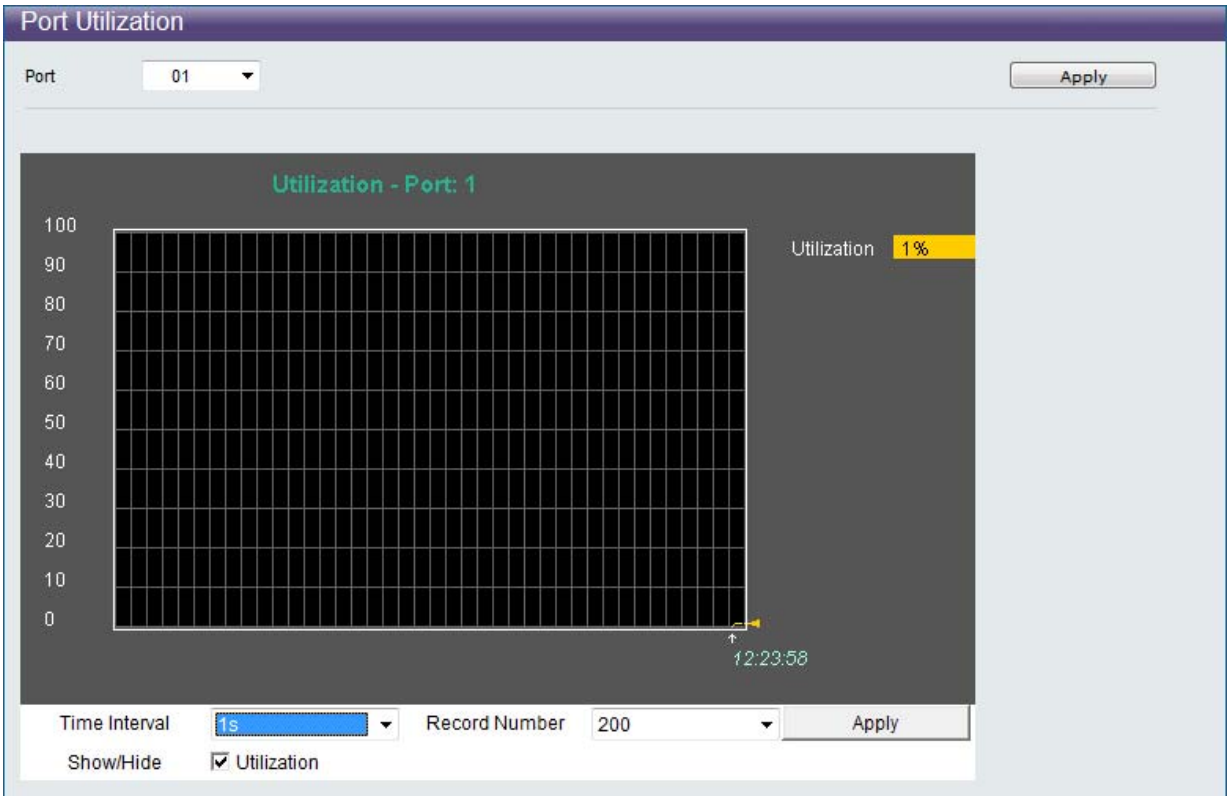


Port Utilization

Users can display the percentage of the total available bandwidth being used on the port.

To view this window, click **Monitoring > Utilization > Port Utilization** as shown below:

Figure 278: Port Utilization window



To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Port Util.

Click the **Apply** button to accept the changes made for each individual section.

Statistics

Port Statistics

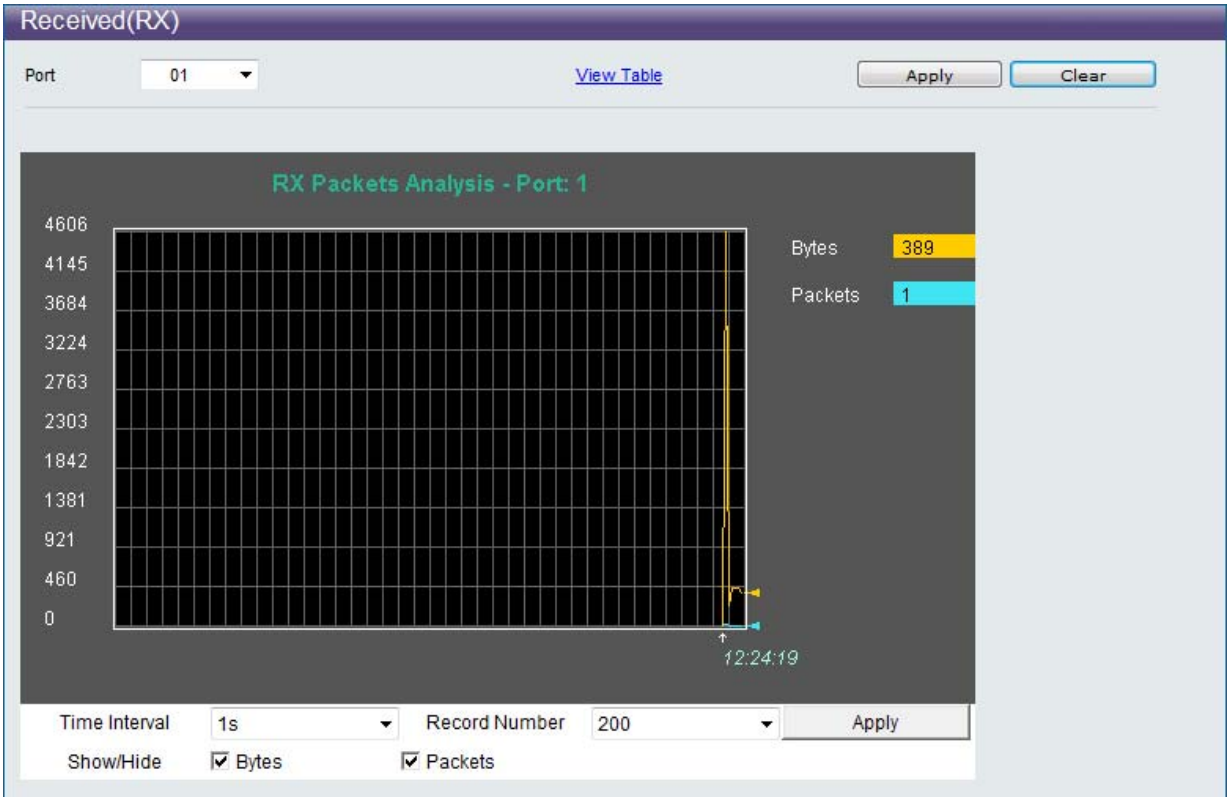
Packets

The Web manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX). To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

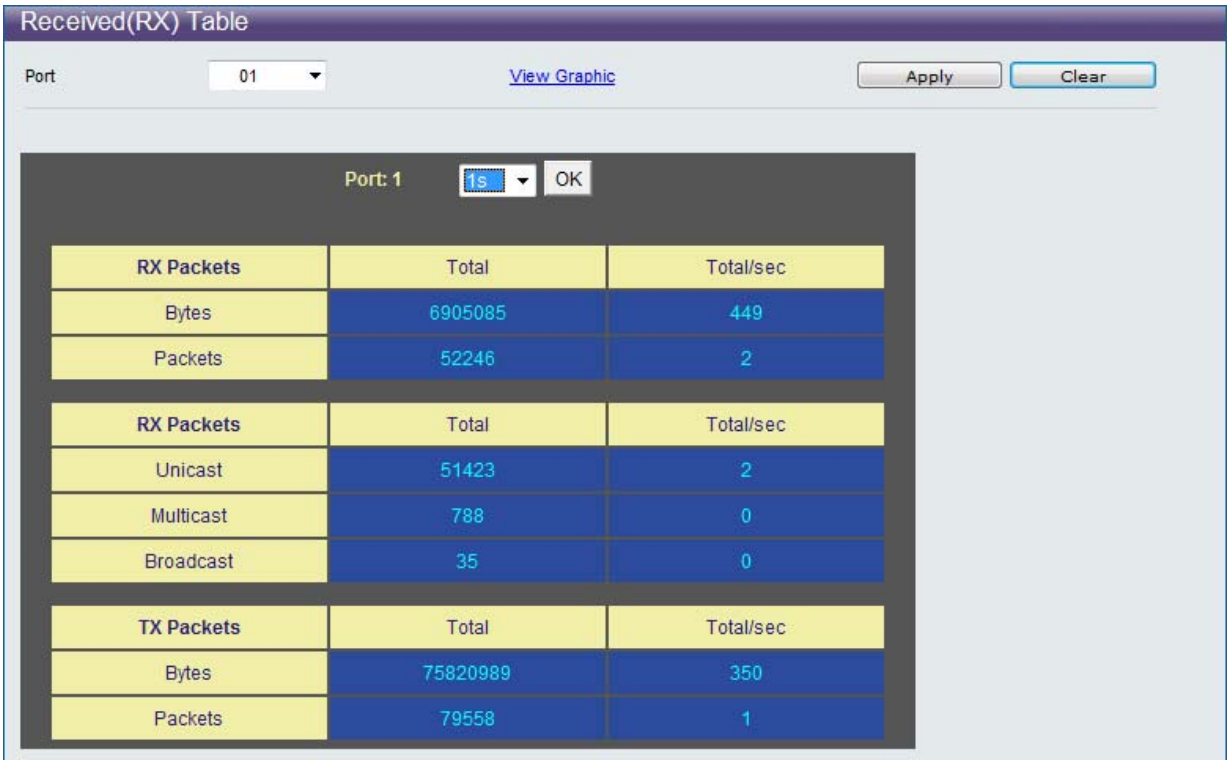
To view this window, click **Monitoring > Statistics > Port Statistics > Packets > Received (RX)** as shown below:

Figure 279: Received (RX) window (for Bytes and Packets)



Click the **View Table** link to display the information in a table rather than a line graph.

Figure 280: RX Packets Analysis Table window



The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

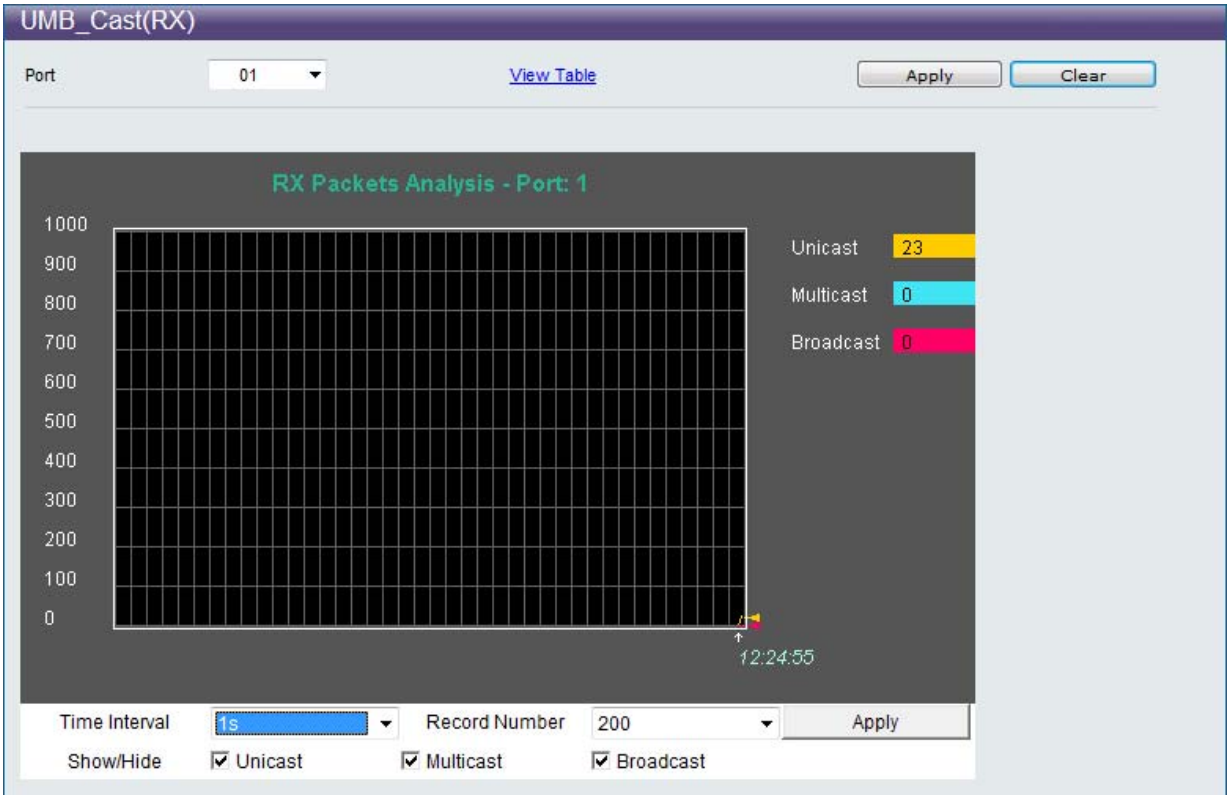
Click the **View Table** link to display the information in a table rather than a line graph.

Click the **View Graphic** link to display the information in a line graph rather than a table.

UMB_Cast (RX). To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

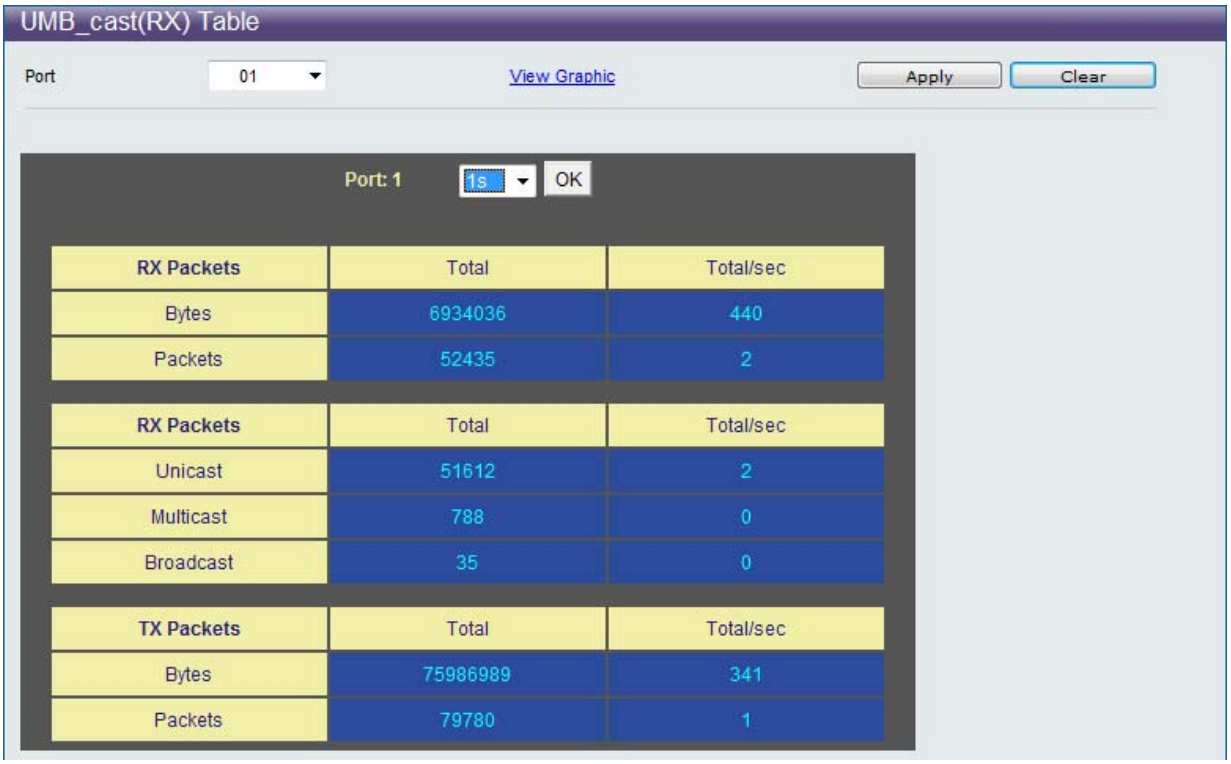
To view this window, click **Monitoring > Statistics > Port Statistics > Packets > UMB_Cast (RX)** as shown below:

Figure 281: UMB_cast (RX) window (for Unicast, Multicast, and Broadcast Packets)



Click the **View Table** link to display the information in a table rather than a line graph.

Figure 282: RX Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)



The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

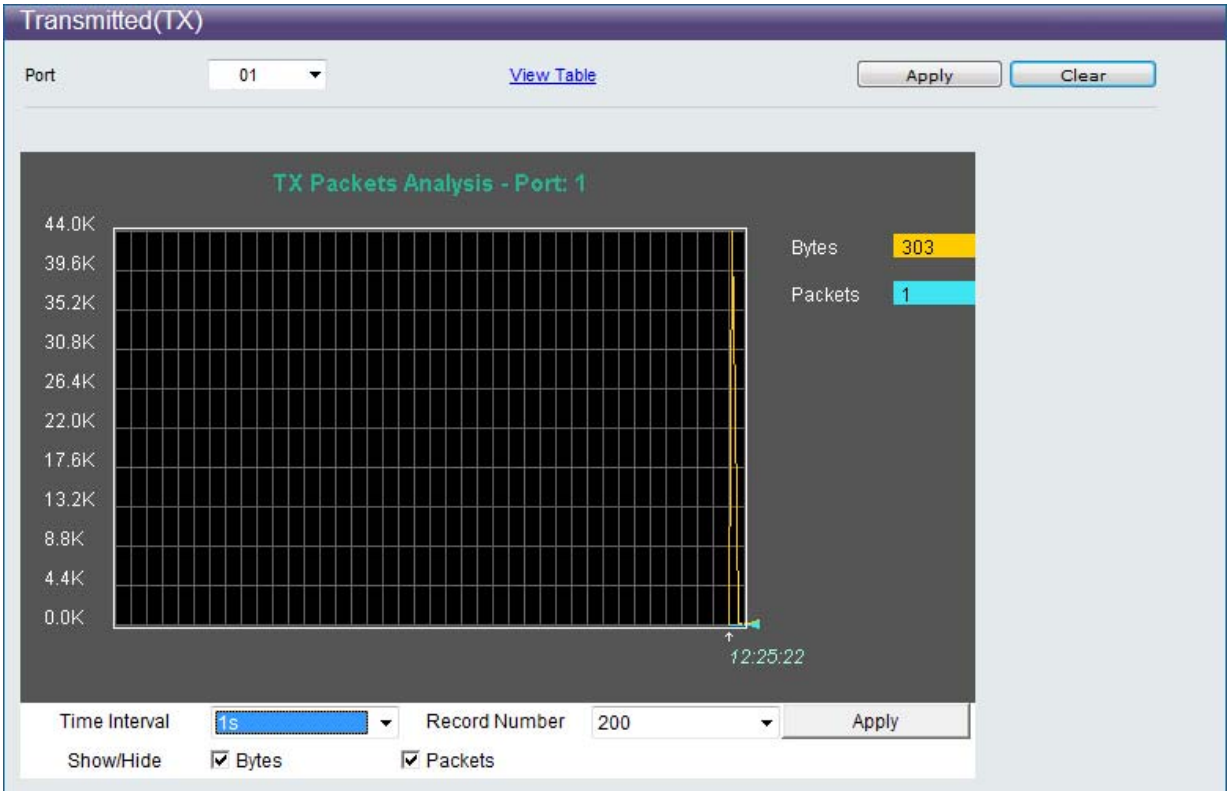
Click the **View Table** link to display the information in a table rather than a line graph.

Click the **View Graphic** link to display the information in a line graph rather than a table.

Transmitted (TX). To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

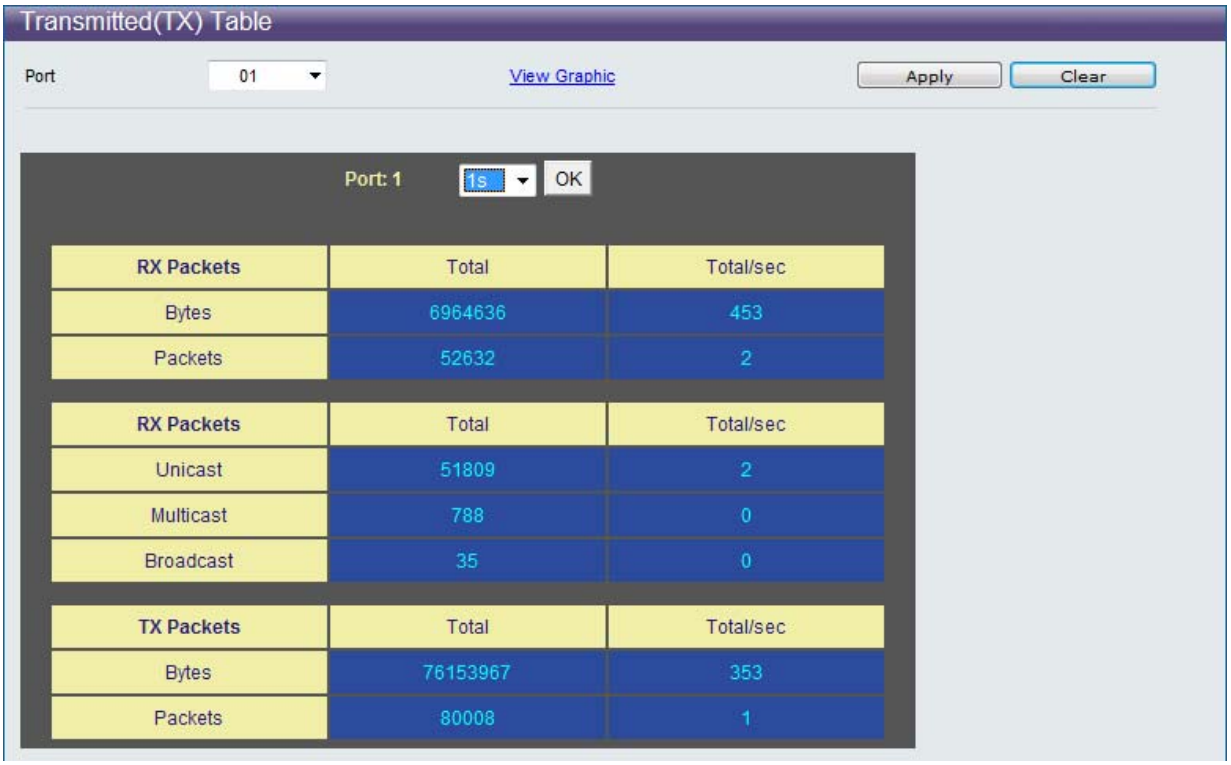
To view this window, click **Monitoring > Statistics > Port Statistics > Packets > Transmitted (TX)** as shown below:

Figure 283: Transmitted (TX) window (for Bytes and Packets)



Click the **View Table** link to display the information in a table rather than a line graph.

Figure 284: TX Packets Analysis window (table for Bytes and Packets)



The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent on the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the **View Table** link to display the information in a table rather than a line graph.

Click the **View Graphic** link to display the information in a line graph rather than a table.

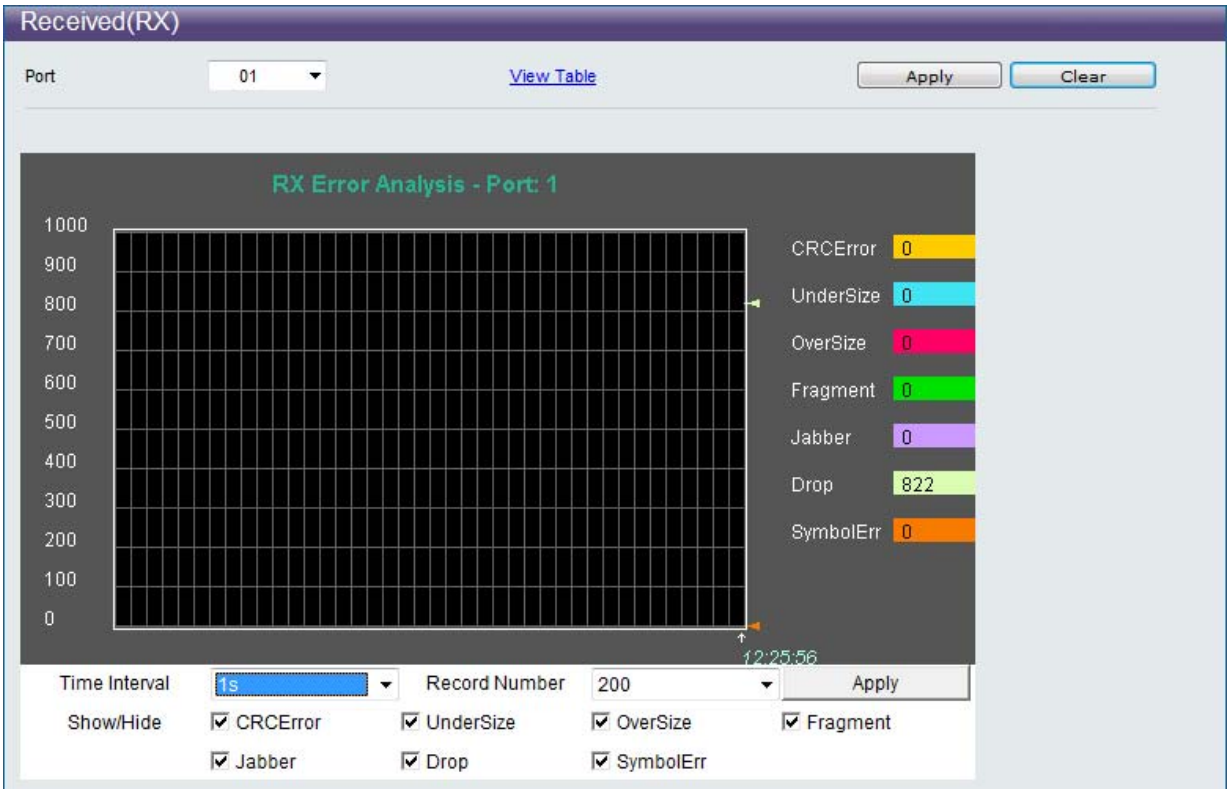
Errors

The Web manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX). To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

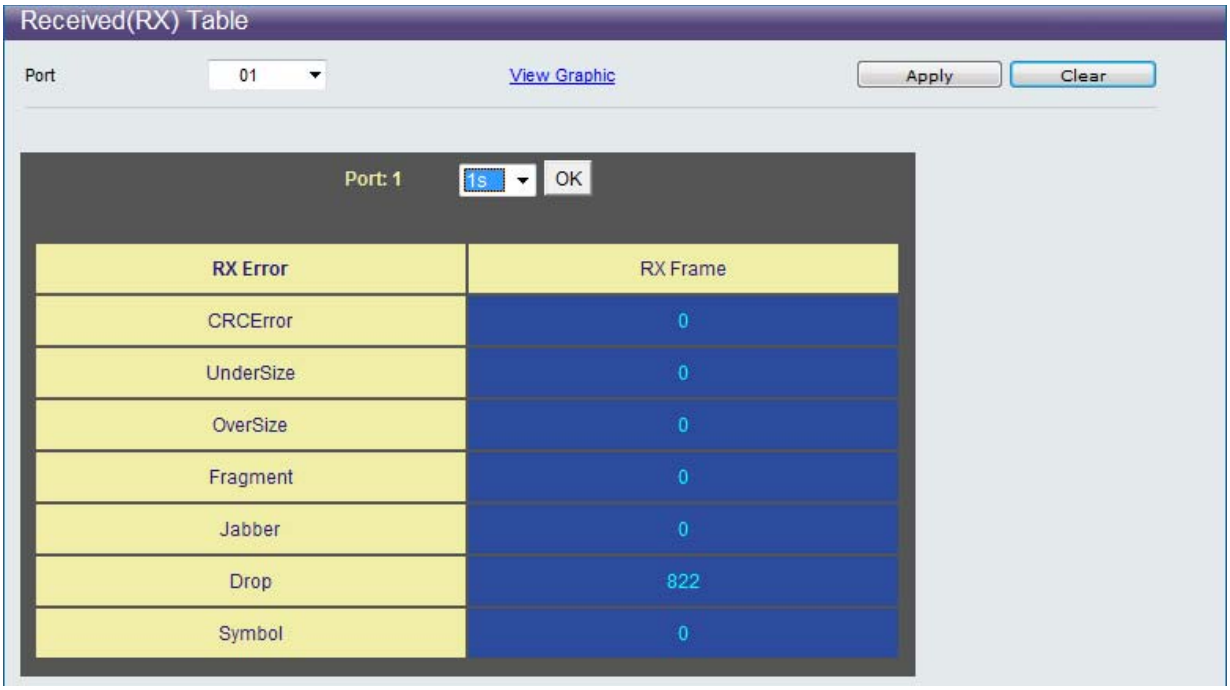
To view this window, click **Monitoring > Statistics > Port Statistics > Errors > Received (RX)** as shown below:

Figure 285: Received (RX) window (for errors)



Click the **View Table** link to display the information in a table rather than a line graph.

Figure 286: RX Error Analysis window (table)



The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
CRCError	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Symbol	Counts the number of packets received that have errors received in the symbol on the physical labor.
Show/Hide	Check whether or not to display CRCError, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

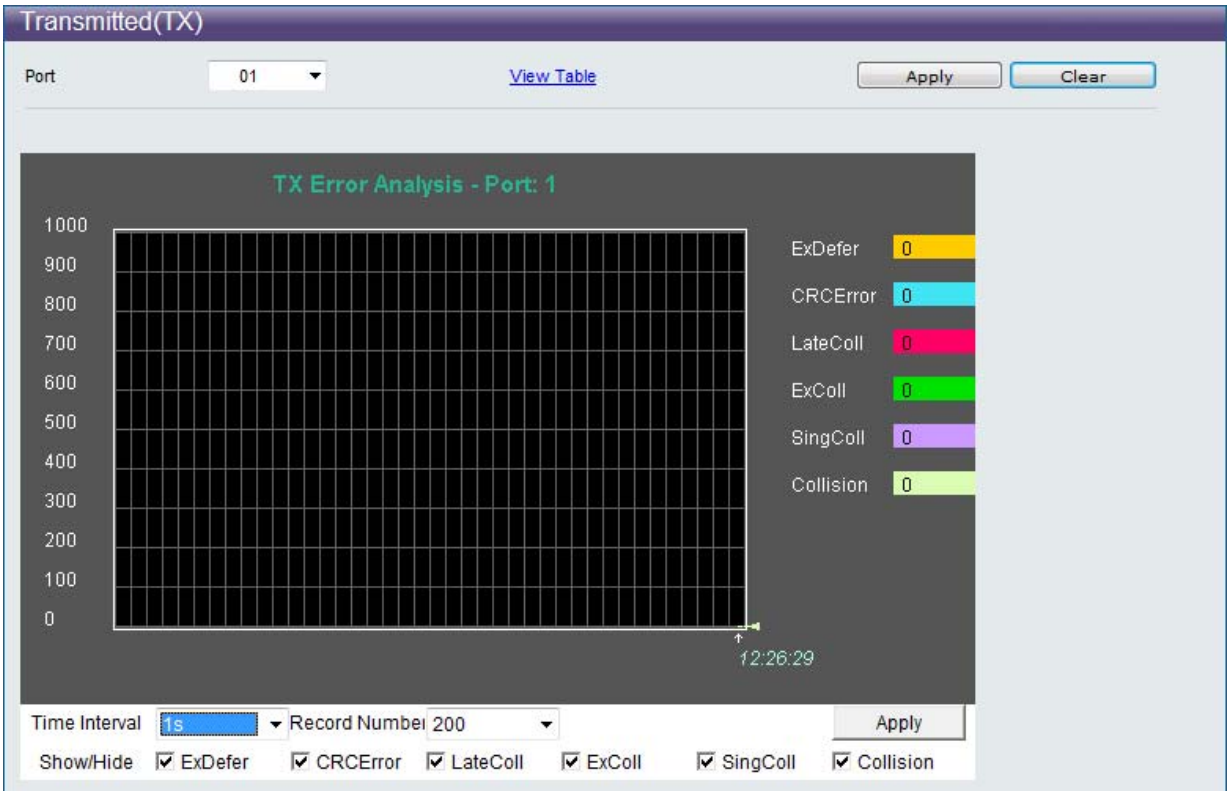
Click the **View Table** link to display the information in a table rather than a line graph.

Click the **View Graphic** link to display the information in a line graph rather than a table.

Transmitted (TX). To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

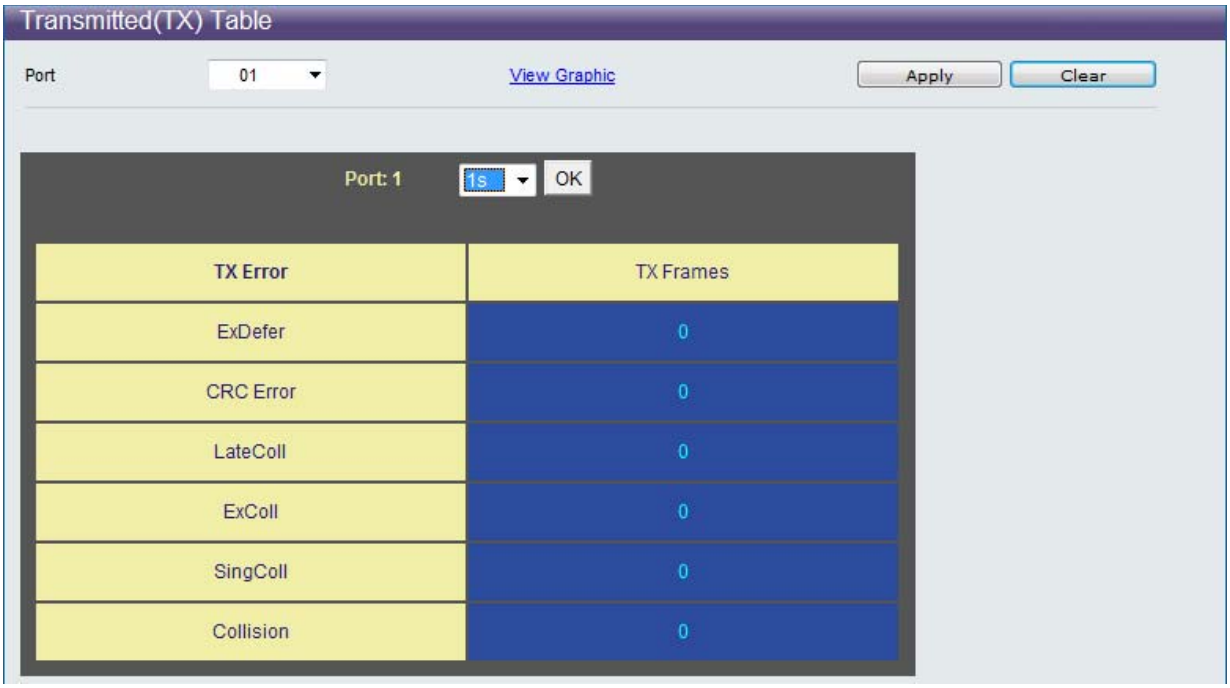
To view this window, click **Monitoring > Statistics > Port Statistics > Errors > Transmitted (TX)** as shown below:

Figure 287: Transmitted (TX) window (for errors)



Click the **View Table** link to display the information in a table rather than a line graph.

Figure 288: TX Error Analysis window (table)



The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the **View Table** link to display the information in a table rather than a line graph.

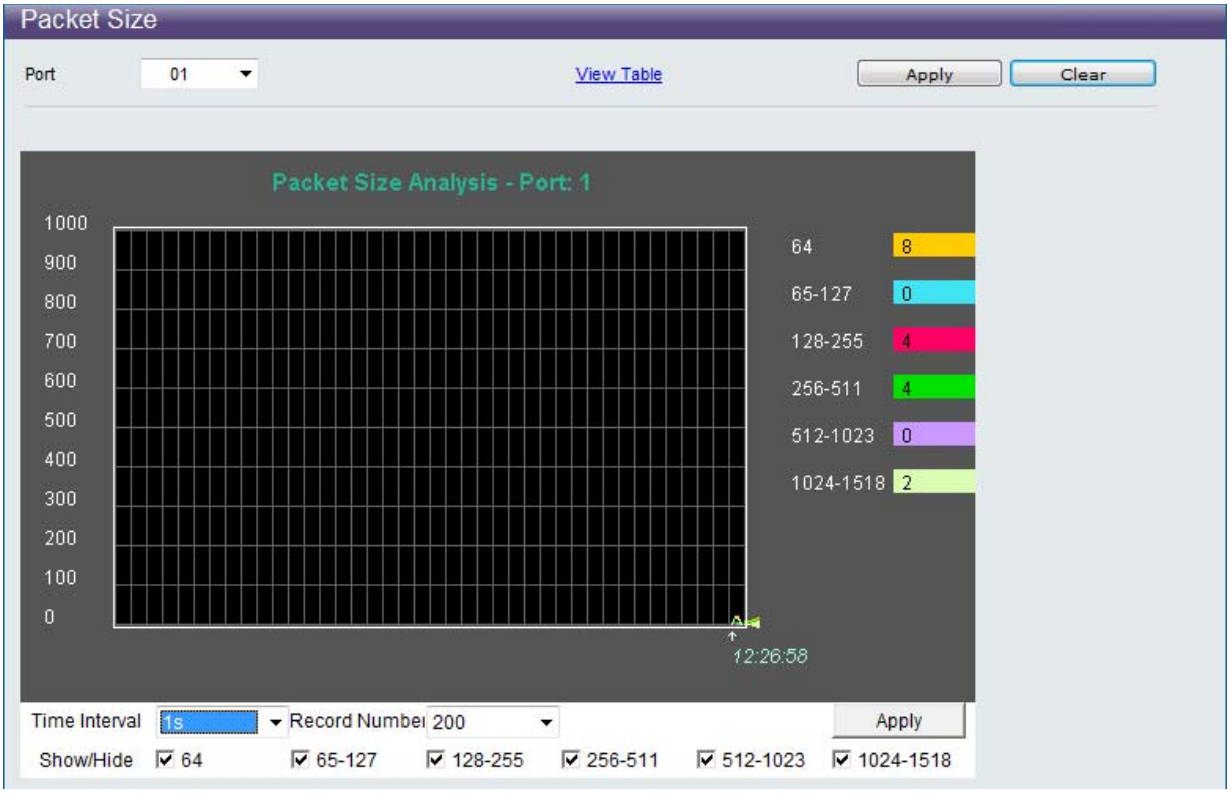
Click the **View Graphic** link to display the information in a line graph rather than a table.

Packet Size

Users can display packets received by the Switch, arranged in six groups and classed by size, as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

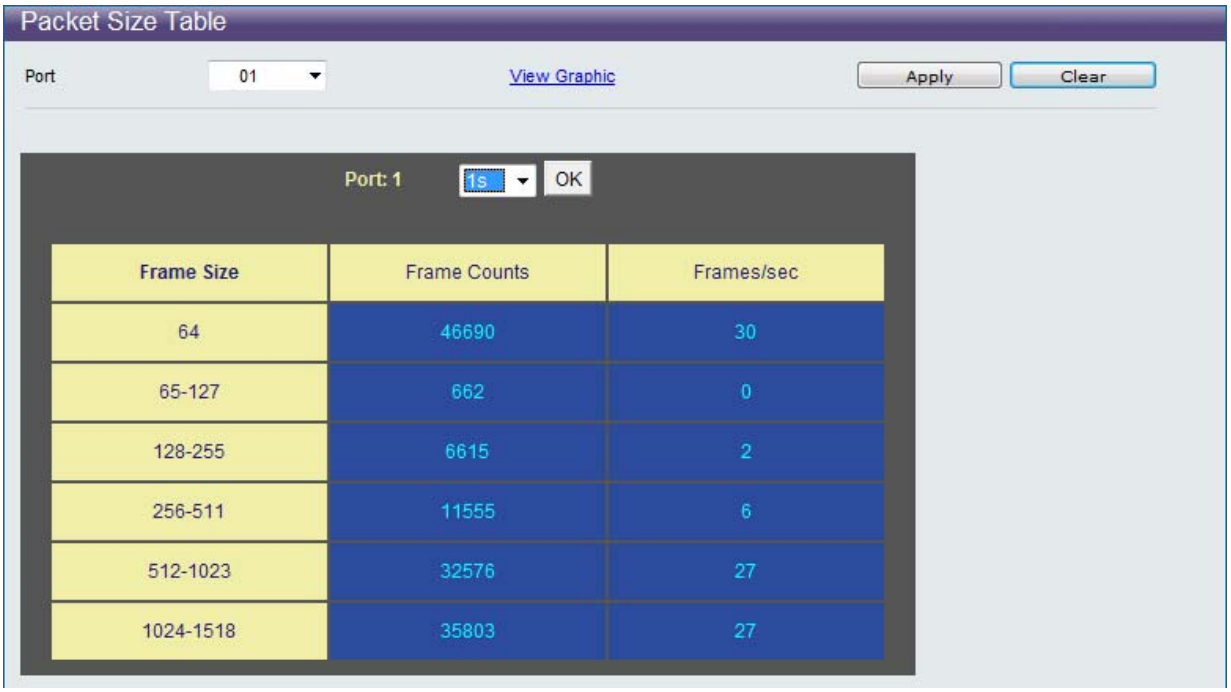
To view this window, click **Monitoring > Statistics > Packet Size** as shown below:

Figure 289: Packet Size window



Click the **View Table** link to display the information in a table rather than a line graph.

Figure 290: RX Size Analysis window (table)



The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the **View Table** link to display the information in a table rather than a line graph.

Click the **View Graphic** link to display the information in a line graph rather than a table.

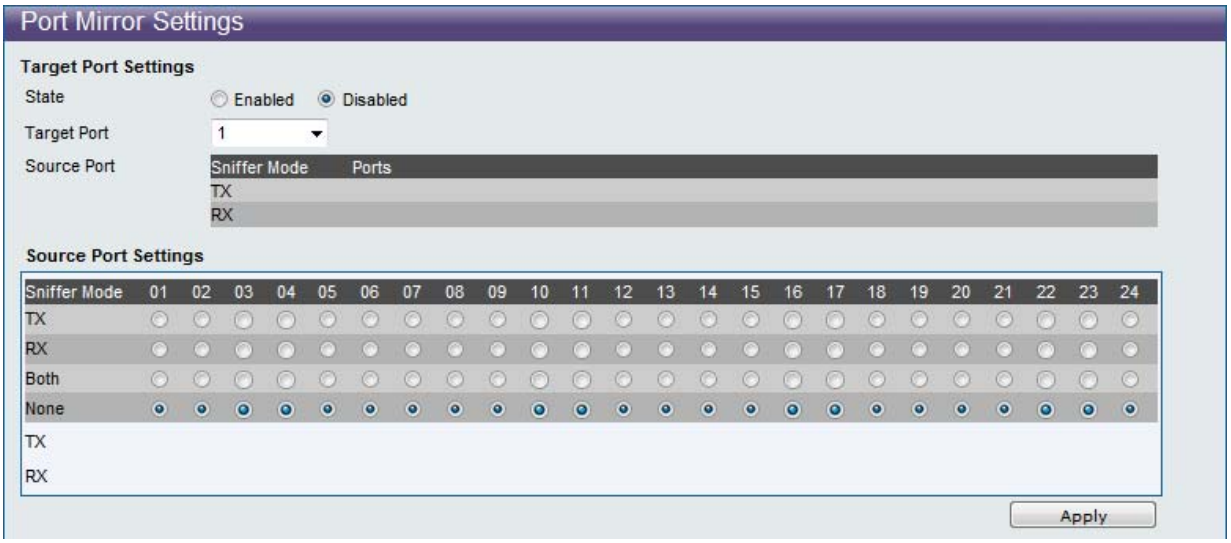
Mirror

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

Port Mirror Settings

To view this window, click **Monitoring > Mirror > Port Mirror Settings** as shown below:

Figure 291: Port Mirror Settings window



The fields that can be configured are described below:

Parameter	Description
State	Click the radio buttons to enable or disable the Port Mirroring feature.
Target Port	Use the drop-down menu to select the Target Port used for Port Mirroring.
TX (Egress)	Click the radio buttons to select whether the port should include outgoing traffic.
RX (Ingress)	Click the radio buttons to select whether the port should include incoming traffic.
Both	Click the radio buttons to select whether the port should include both incoming and outgoing traffic.

Parameter	Description
None	Click the radio buttons to select whether the port should not include any traffic.

Click the **Apply** button to accept the changes made.

NOTE

You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Please note a target port and a source port cannot be the same port.

RSPAN Settings

This page controls the RSPAN function. The purpose of the RSPAN function is to mirror packets to a remote switch. A packet travels from the switch where the monitored packet is received, passing through the intermediate switch, and then to the switch where the sniffer is attached. The first switch is also named the source switch.

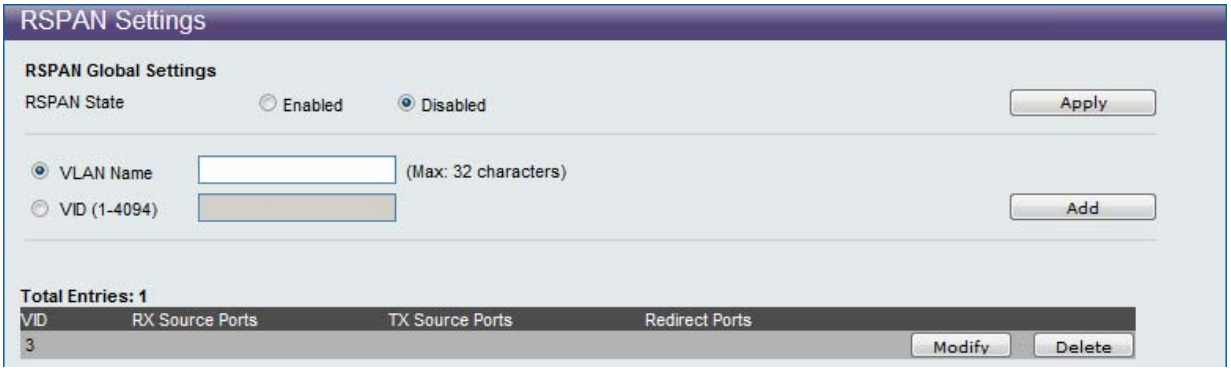
To make the RSPAN function work, the RSPAN VLAN source setting must be configured on the source switch. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured.

NOTE

RSPAN VLAN mirroring will only work when RSPAN is enabled (when one RSPAN VLAN has been configured with a source port). The RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

To view this window, click **Monitoring > Mirror > RSPAN Settings** as shown below:

Figure 292: RSPAN Settings window



The fields that can be configured are described below:

Parameter	Description
RSPAN State	Click the radio buttons to enable or disable the RSPAN feature.

Parameter	Description
VLAN Name	Create the RSPAN VLAN by VLAN name.
VID	Create the RSPAN VLAN by VLAN ID.

Click the **Apply** button to accept the changes made.

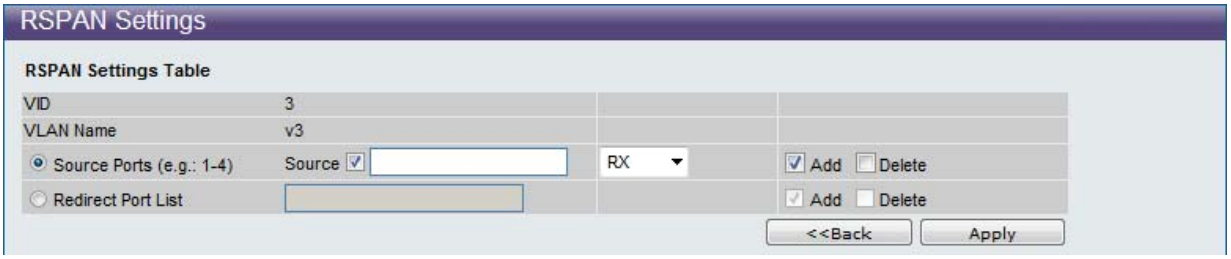
Click the **Add** button to add a new entry based on the information entered.

Click the **Modify** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Modify** button, the following page will appear:

Figure 293: RSPAN Settings – Modify window



The fields that can be configured are described below:

Parameter	Description
VID	Displays the RSPAN VLAN by VLAN ID.
VLAN Name	Displays the RSPAN VLAN by VLAN name.
Source Ports	If the ports are not specified by option, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters. Select **RX, TX** or **Both** to specify in which direction the packets will be monitored. Tick **Add** or **Delete** to add or delete source ports.
Redirect Port List	Specify the output port list for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, the Link Aggregation behavior will apply to the RSPAN packets. Tick **Add** or **Delete** to add or delete redirect ports.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

sFlow

sFlow (RFC3176) is a technology for monitoring traffic in data networks containing switches and routers. The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The architecture and sampling techniques used in the

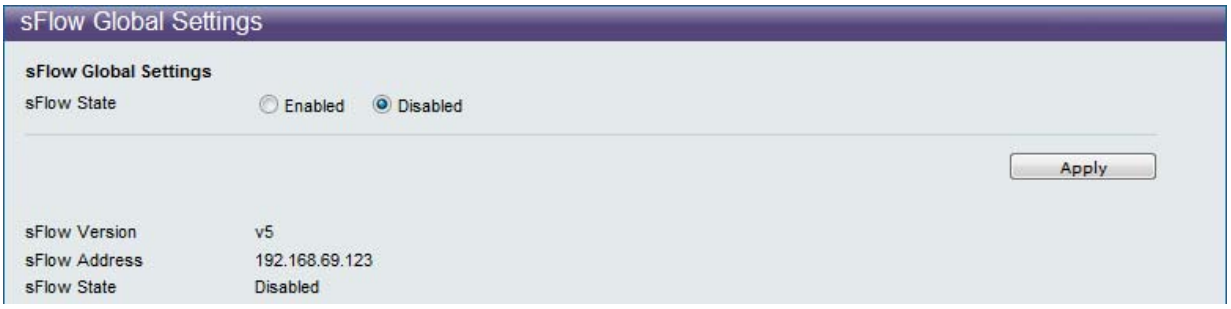
sFlow monitoring system were designed for providing continuous site-wide (and enterprise-wide) traffic monitoring of high speed switched and routed networks.

sFlow Global Settings

This window is used to enable or disable the sFlow feature.

To view this window, click **Monitoring > sFlow > sFlow Global Settings** as shown below:

Figure 294: sFlow Global Settings window



The fields that can be configured are described below:

Parameter	Description
sFlow State	Here the user can enable or disable the sFlow feature.

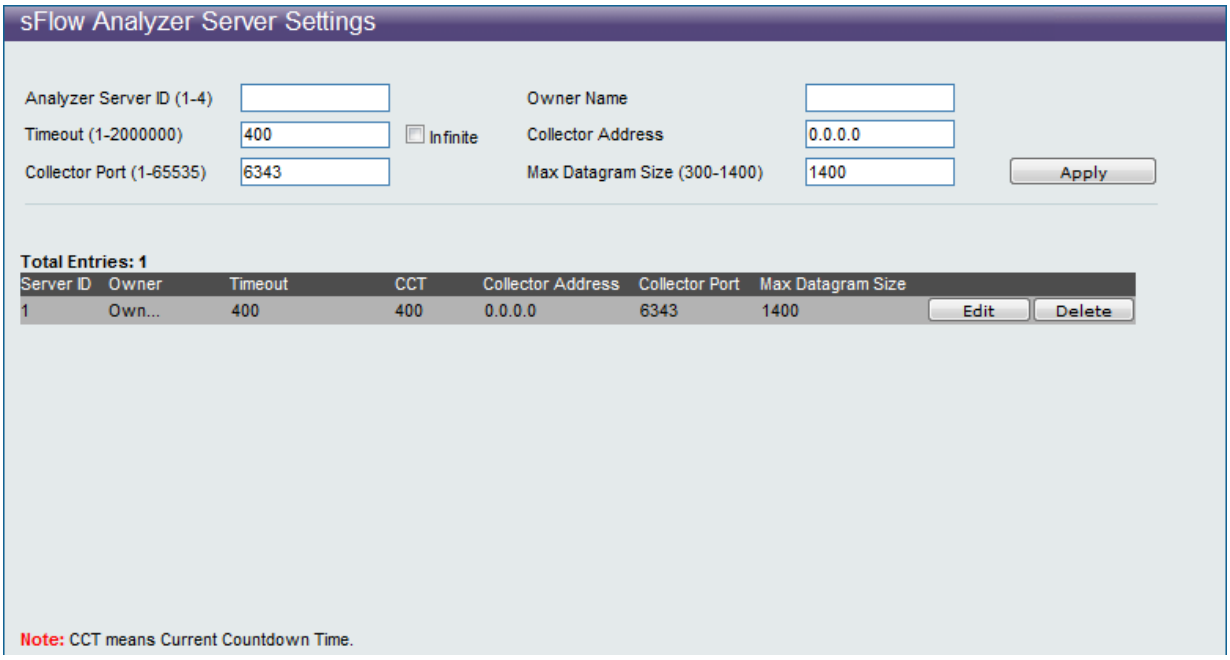
Click the **Apply** button to accept the changes made.

sFlow Analyzer Server Settings

The Switch can support 4 different Analyzer Servers at the same time and each sampler or poller can select a collector to send the samples. We can send different samples from different samplers or pollers to different collectors.

To view this window, click **Monitoring > sFlow > sFlow Analyzer Server Settings** as shown below:

Figure 295: sFlow Analyzer Server Settings window



The fields that can be configured are described below:

Parameter	Description
Analyzer Server ID	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Owner Name	The entity making use of this sFlow analyzer server. When owner is set or modified, the timeout value will become 400 automatically.
Timeout	The length of time before the server times out. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted. If not specified, its default value is 400.
Collector Address	The IP address of the analyzer server. If not specified or set a 0 address, the entry will be inactive.
Collector Port	The destination UDP port for sending the sFlow datagrams. If not specified, the default value is *6343*.
Max Datagram Size	The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

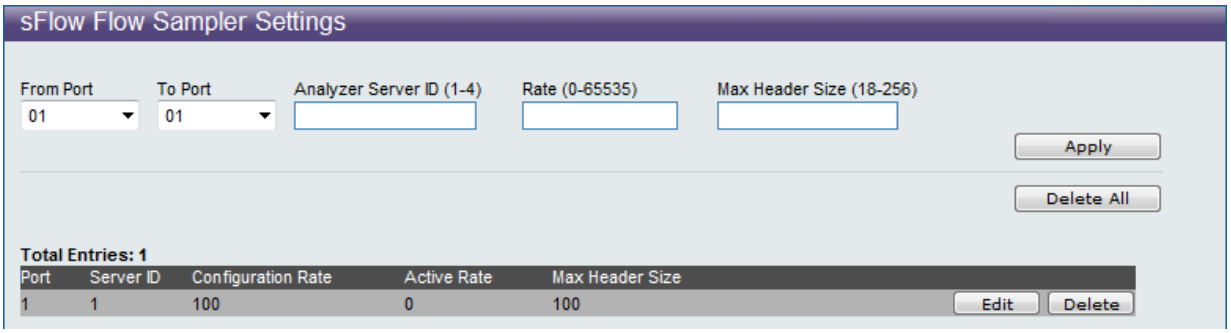
sFlow Flow Sampler Settings

On this page the user can configure the sFlow flow sampler parameters. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at the specified interval.

NOTE

If the user wants the change the analyze server ID, he needs to delete the flow sampler and creates a new one.

Figure 296: sFlow Flow Sampler Settings window



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to specify the list of ports to be configured.
Analyzer Server ID	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Rate	The sampling rate for packet Rx sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. The sampling rate for packet Tx sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.
MAX Header Size	The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

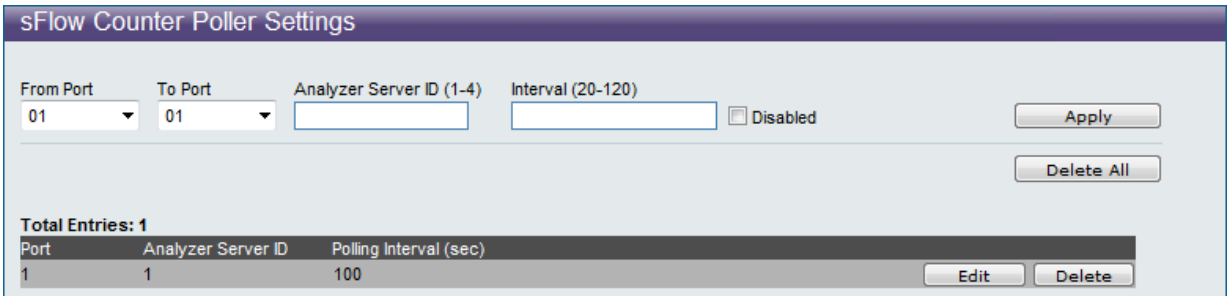
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

sFlow Counter Poller Settings

On this page the user can configure the sFlow counter poller parameters. If the user wants to change the analyzer server ID, he needs to delete the counter poller and create a new one.

Figure 297: sFlow Counter Poller Settings



The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to specify the list of ports to be configured.
Analyzer Server ID	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Interval	The maximum number of seconds between successive samples of the counters.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

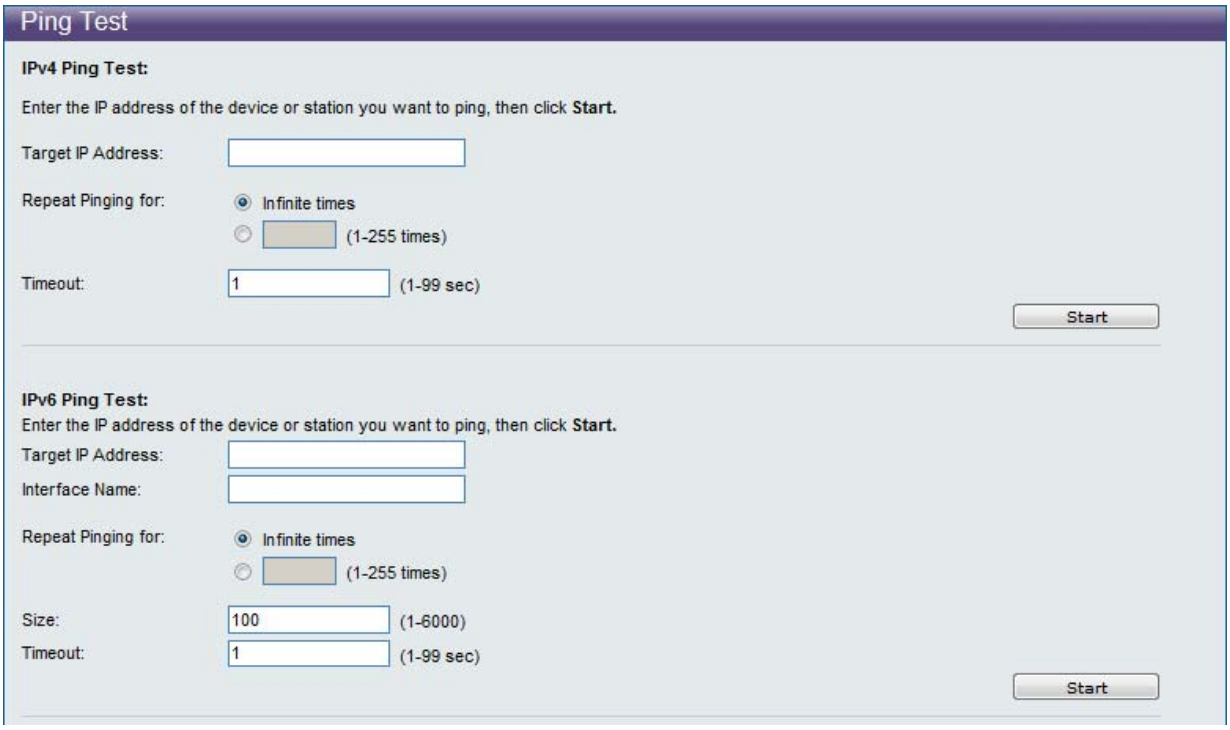
Click the **Delete** button to remove the specific entry.

Ping Test

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To view this window, click **Monitoring > Ping Test** as shown below:

Figure 298: Ping Test window



The user may click the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between *1* and *255*.

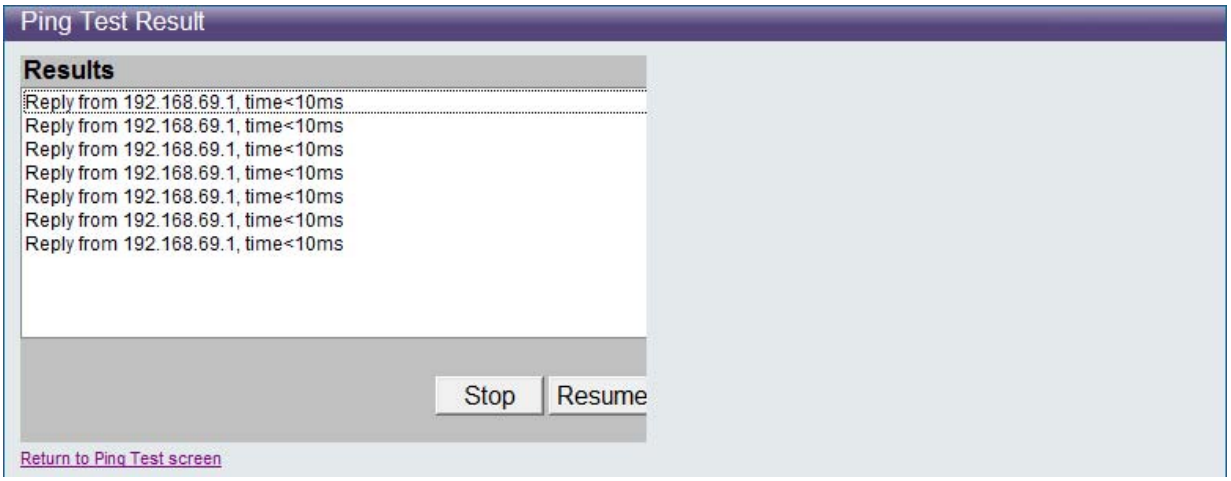
The fields that can be configured are described below:

Parameter	Description
Target IP Address	Enter an IP address to be pinged.
Repeat Pinging for	Enter the number of times desired to attempt to Ping either the IPv4 address or the IPv6 address configured in this window. Users may enter a number of times between *1* and *255*.
Size	For IPv6 only, enter a value between *1* and *6000*. The default is *100*.
Timeout	Select a timeout period between *1* and *99* seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

Click the **Start** button to initiate the Ping Test.

After clicking the **Start** button, the following page will appear:

Figure 299: Ping Test Result window



Click the **Stop** button to halt the Ping Test.

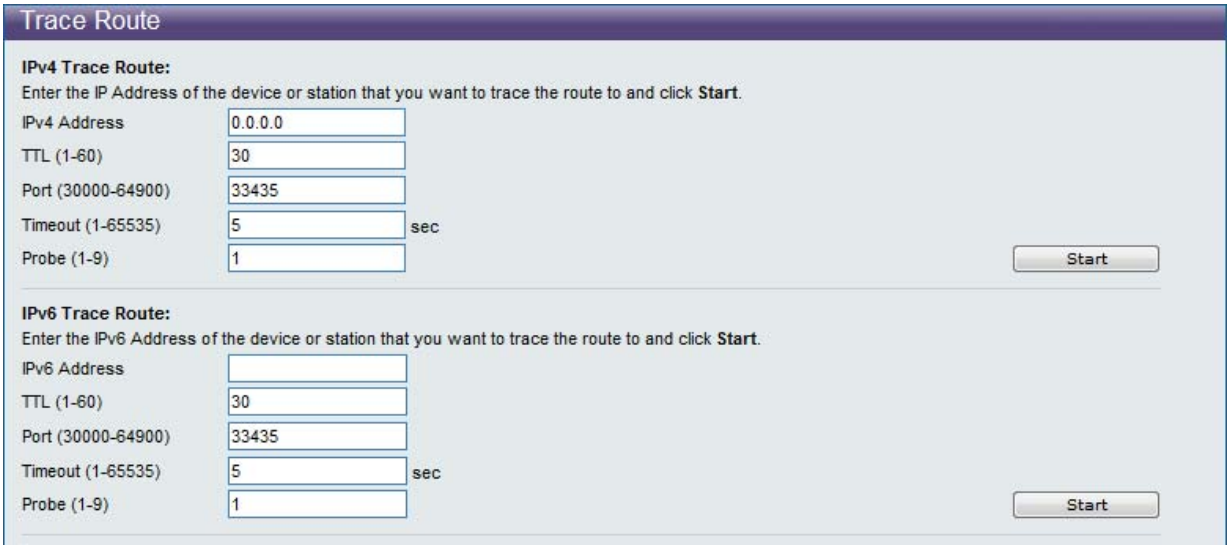
Click the **Resume** button to resume the Ping Test.

Trace Route

The trace route page allows the user to trace a route between the switch and a given host on the network.

To view this window, click **Monitoring > Trace Route** as shown below:

Figure 300: Trace Route window


Trace Route
IPv4 Trace Route:
Enter the IP Address of the device or station that you want to trace the route to and click Start.
IPv4 Address 0.0.0.0
TTL (1-60) 30
Port (30000-64900) 33435
Timeout (1-65535) 5 sec
Probe (1-9) 1
Start
IPv6 Trace Route:
Enter the IPv6 Address of the device or station that you want to trace the route to and click Start.
IPv6 Address
TTL (1-60) 30
Port (30000-64900) 33435
Timeout (1-65535) 5 sec
Probe (1-9) 1
Start

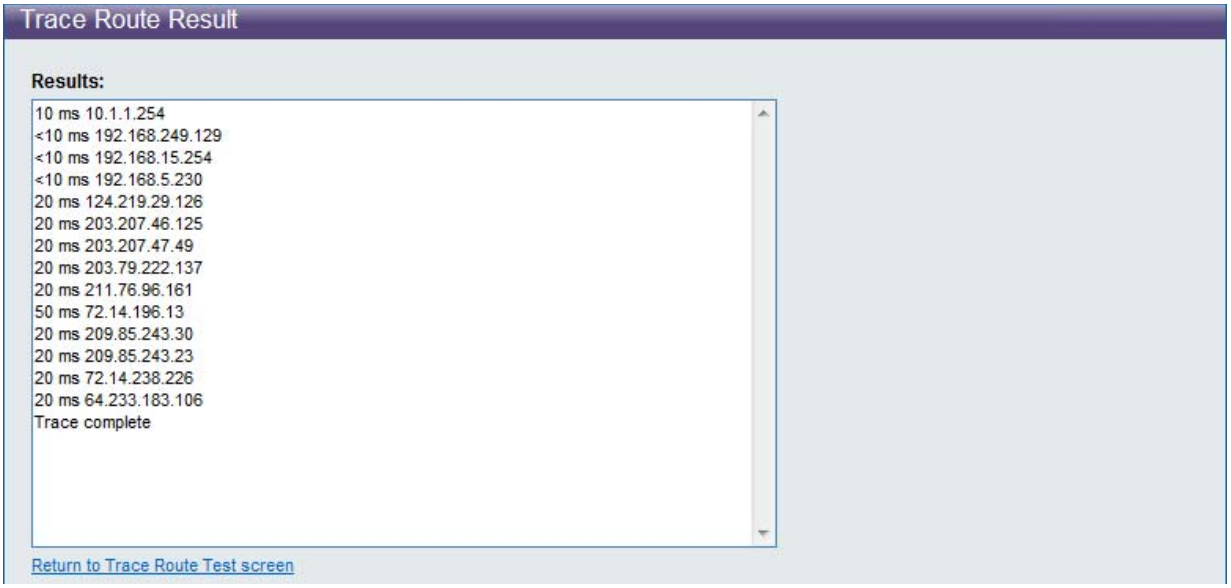
The fields that can be configured are described below:

Parameter	Description
IPv4 Address / IPv6 Address	IP address of the destination station.
TTL	The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.
Port	The port number. The value range is from 30000 to 64900.
Timeout	Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Probe	The number of probing. The range is from 1 to 9. If unspecified, the default value is 1.

Click the **Start** button to initiate the Trace Route.

After clicking the **Start** button, the following page will appear:

Figure 301: Trace Route Result window



Click the **Stop** button to halt the Trace Route.

Click the **Resume** button to resume the Trace Route.

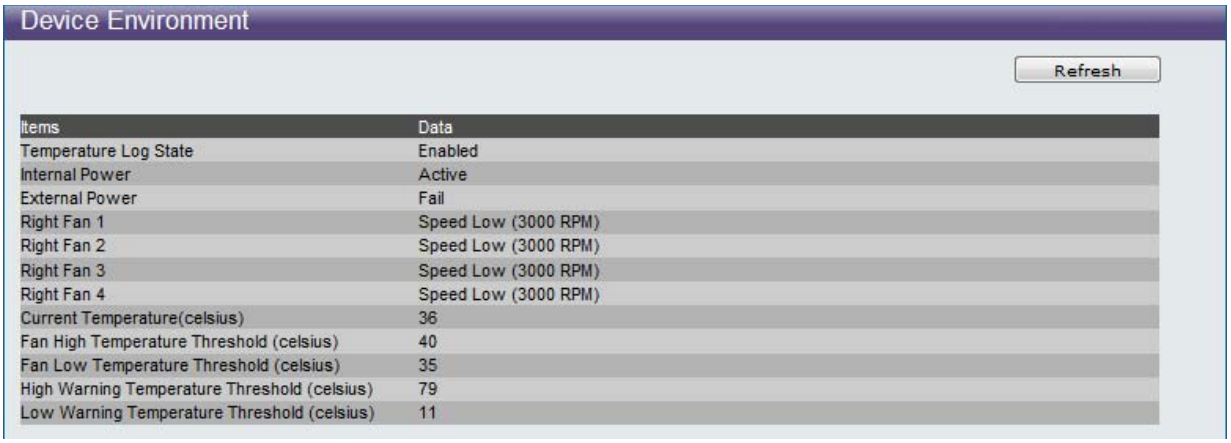
Peripheral

Device Environment

The device environment feature displays the Switch internal temperature status.

To view this window, click **Monitoring > Peripheral > Device Environment** as shown below:

Figure 302: Device Environment window



Click the **Refresh** button to refresh the display table so that new entries will appear.

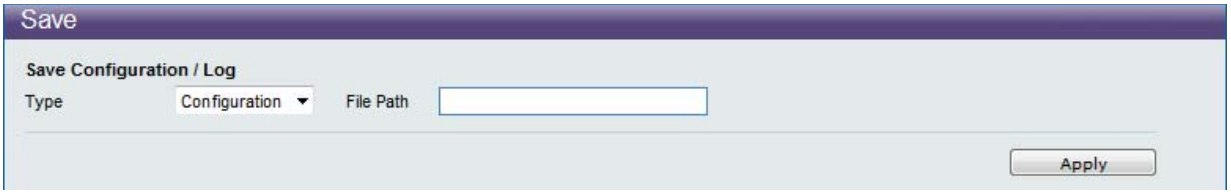
12 CHAPTER Save and Tools

Save Configuration / Log

To view this window, click **Save > Save Configuration / Log**, as shown below.

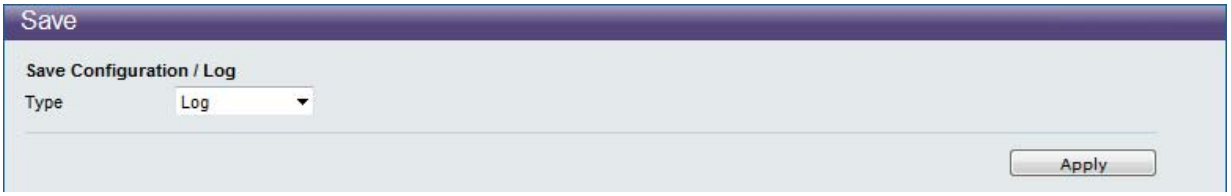
Save Configuration allows the user to backup the configuration of the switch to a folder on the computer. Select **Configuration** from the **Type** drop-down menu and enter the **File Path** in the space provided and click **Apply**.

Figure 303: Save – Configuration window



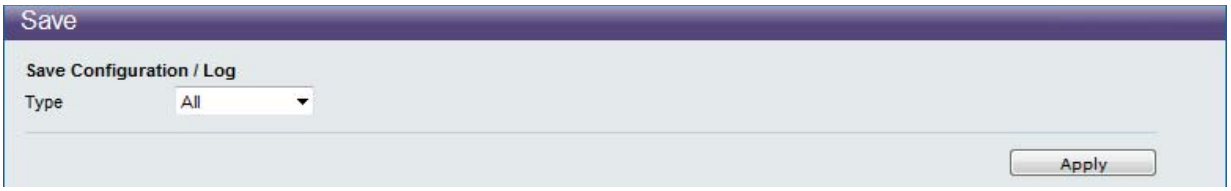
Save Log allows the user to backup the log file of the switch. Select **Log** from the **Type** drop-down menu and click **Apply**.

Figure 304: Save – Log window



Save All allows the user to permanently save changes made to the configuration. This option will allow the changes to be kept after the switch has rebooted. Select **All** from the **Type** drop-down menu and click **Apply**.

Figure 305: Save – All window



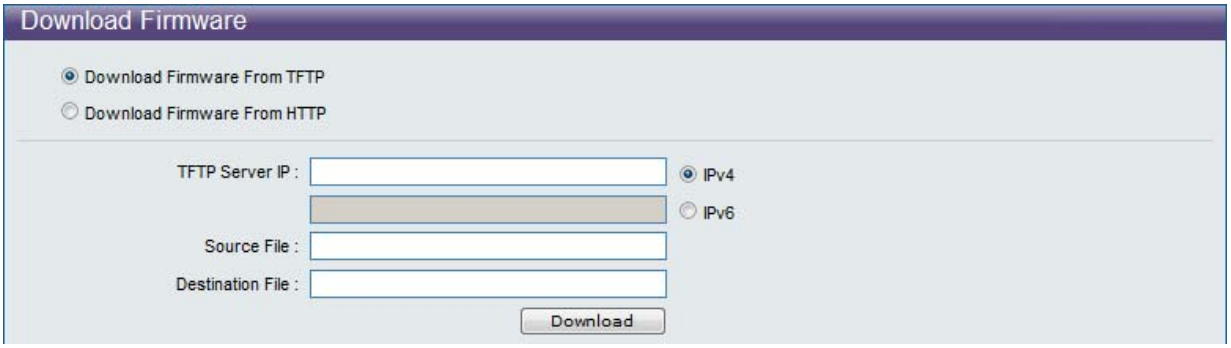
Download firmware

The following window is used to download firmware for the Switch.

Download Firmware From TFTP

This page allows the user to download firmware from a TFTP Server to the Switch and updates the switch.

Figure 306: Download Firmware – TFTP window



The fields that can be configured are described below:

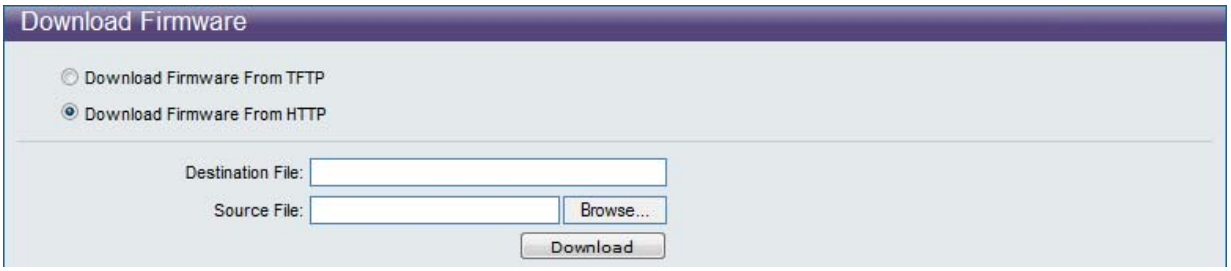
Parameter	Description
TFTP Server IP	Enter the TFTP server IP address used.
	IPv4 Click the radio button to enter the TFTP server IP address used.
	IPv6 Click the radio button to enter the TFTP server IPv6 address used.
Source File	Enter the location and name of the Source File.
Destination File	Enter the location and name of the Destination File.

Click **Download** to initiate the download.

Download Firmware From HTTP

This page allows the user to download firmware from a computer to the Switch and updates the switch.

Figure 307: Download Firmware – HTTP window



The fields that can be configured are described below:

Parameter	Description
Destination File	Enter the location of the Destination File.
Source File	Enter the location of the Source File or click the **Browse** button to navigate to the firmware file for the download.

Click **Download** to initiate the download.

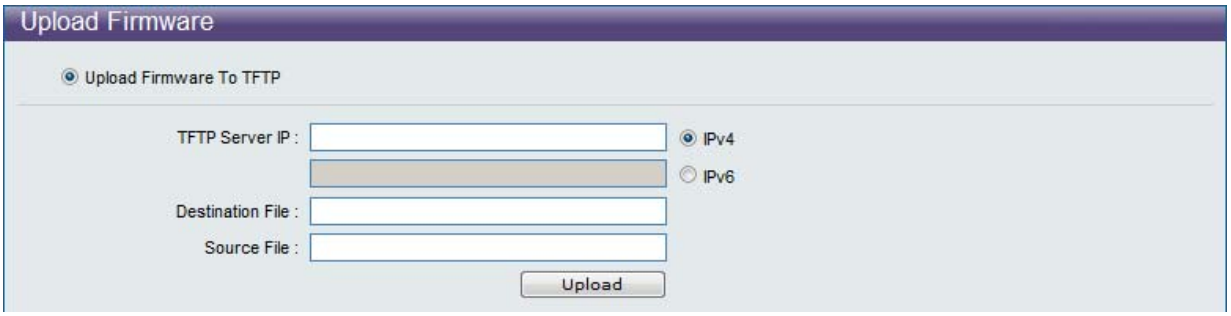
Upload Firmware

The following window is used to upload firmware from the Switch.

Upload Firmware To TFTP

This page allows the user to upload firmware from the Switch to a TFTP Server.

Figure 308: Upload Firmware – TFTP window



The fields that can be configured are described below:

Parameter	Description
TFTP Server IP	Enter the TFTP server IP address used.
	IPv4 Click the radio button to enter the TFTP server IP address used.
	IPv6 Click the radio button to enter the TFTP server IPv6 address used.
Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File.

Click **Upload** to initiate the upload.

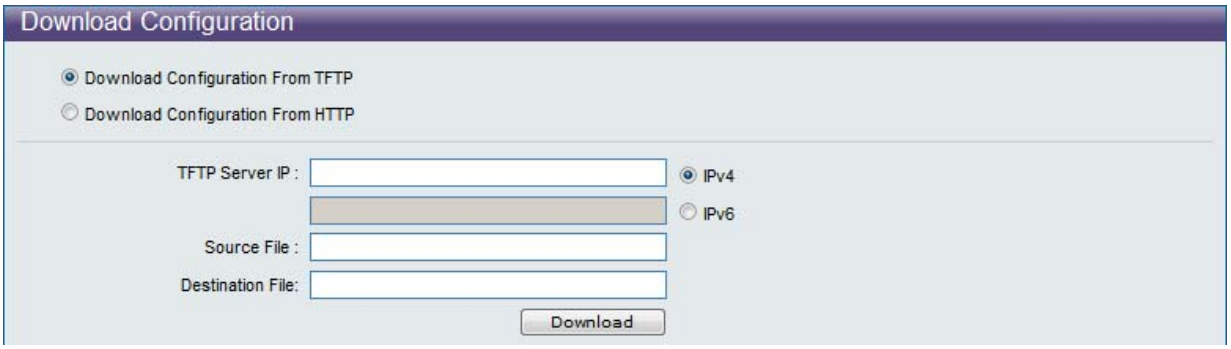
Download Configuration

The following window is used to download the configuration file for the Switch.

Download Configuration From TFTP

This page allows the user to download the configuration file from a TFTP Server to the Switch and updates the switch.

Figure 309: Download Configuration – TFTP window



The fields that can be configured are described below:

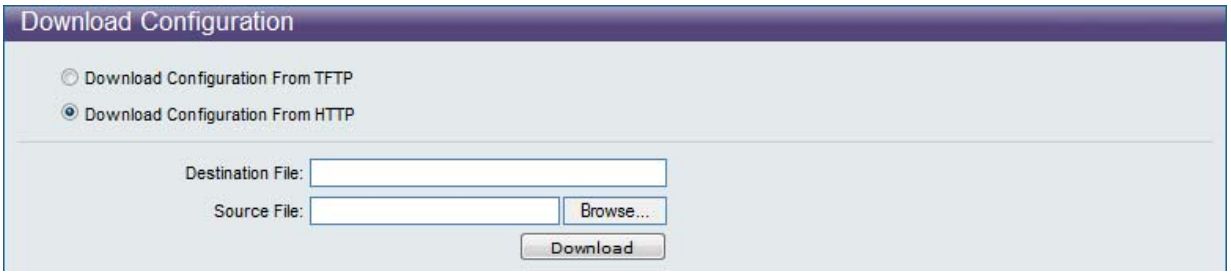
Parameter	Description
TFTP Server IP	Enter the TFTP server IP address used.
	IPv4 Click the radio button to enter the TFTP server IP address used.
	IPv6 Click the radio button to enter the TFTP server IPv6 address used.
Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File.

Click **Download** to initiate the download.

Download Configuration From HTTP

This page allows the user to download the configuration file from a computer to the Switch and updates the switch.

Figure 310: Download Configuration – HTTP window



The fields that can be configured are described below:

Parameter	Description
Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File, or click the **Browse** button to navigate to the configuration file for the download.

Click **Download** to initiate the download.

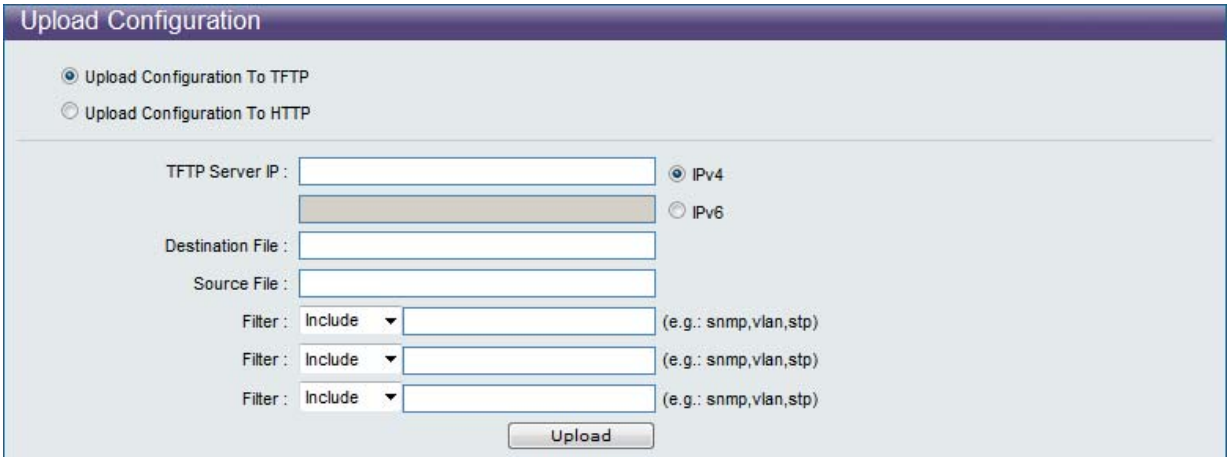
Upload Configuration

The following window is used to upload the configuration file from the Switch.

Upload Configuration To TFTP

This page allows the user to upload the configuration file from the Switch to a TFTP Server.

Figure 311: Upload Configuration – TFTP window



The fields that can be configured are described below:

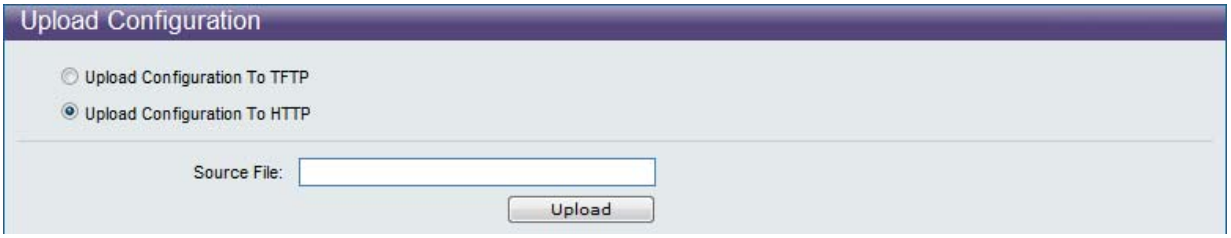
Parameter	Description
TFTP Server IP	Enter the TFTP server IP address used.
	IPv4 Click the radio button to enter the TFTP server IP address used.
	IPv6 Click the radio button to enter the TFTP server IPv6 address used.
Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File.
Filter	Use the drop-down menu to *include, begin* or *exclude* a filter like SNMP, VLAN or STP. Select the appropriate **Filter** action and enter the service name in the space provided.

Click **Upload** to initiate the upload.

Upload Configuration To HTTP

This page allows the user to upload the configuration file from the Switch to a computer.

Figure 312: Upload Configuration – HTTP window



The fields that can be configured are described below:

Parameter	Description

Parameter	Description
Source File	Enter the location and name of the Source File.

Click **Upload** to initiate the upload.

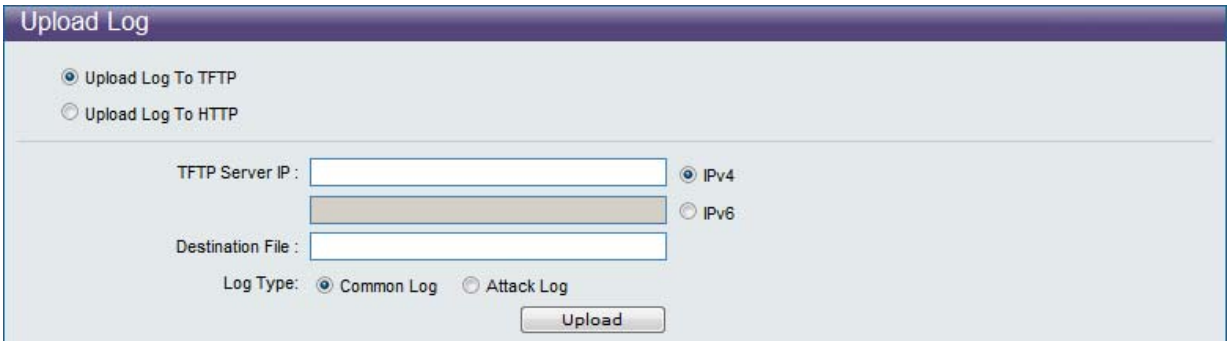
Upload Log File

The following window is used to upload the log file from the Switch.

Upload Log To TFTP

This page allows the user to upload the log file from the Switch to a TFTP Server.

Figure 313: Upload Log – TFTP window



The fields that can be configured are described below:

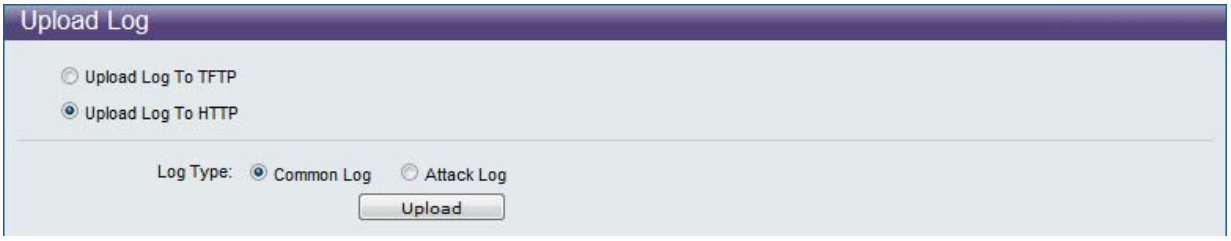
Parameter	Description
TFTP Server IP	Enter the TFTP server IP address used.
	IPv4 Click the radio button to enter the TFTP server IP address used.
	IPv6 Click the radio button to enter the TFTP server IPv6 address used.
Destination File	Enter the location and name of the Destination File.
Log Type	Select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Upload Log To HTTP

This page allows the user to upload the log file from the Switch to a computer.

Figure 314: Upload Log – HTTP window



The fields that can be configured are described below:

Parameter	Description
Log Type	Here the user can select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.

Click **Upload** to initiate the upload.

Reset

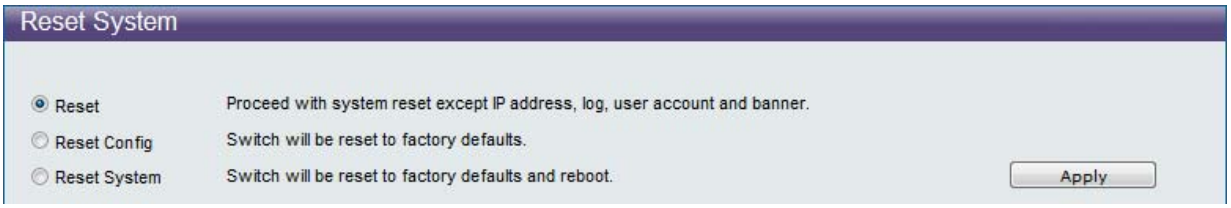
The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

NOTE

Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factor.

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

Figure 315: Reset System window


Reset System
Reset
Proceed with system reset except IP address, log, user account and banner.
Reset Config
Switch will be reset to factory defaults.
Reset System
Switch will be reset to factory defaults and reboot.
Apply

The fields that can be configured are described below:

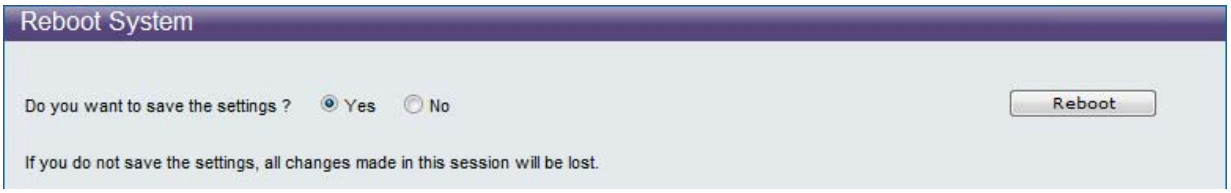
Parameter	Description
Reset	Selecting this option will factory reset the Switch but not the *IP Address, User Accounts* and the *Banner*.
Reset Config	Selecting this option will factory reset the Switch but not perform a Reboot.
Reset System	Selecting this option will factory reset the Switch and perform a Reboot.

Click the **Apply** button to initiate the Reset action.

Reboot System

The following window is used to restart the Switch.

Figure 316: Reboot System Window

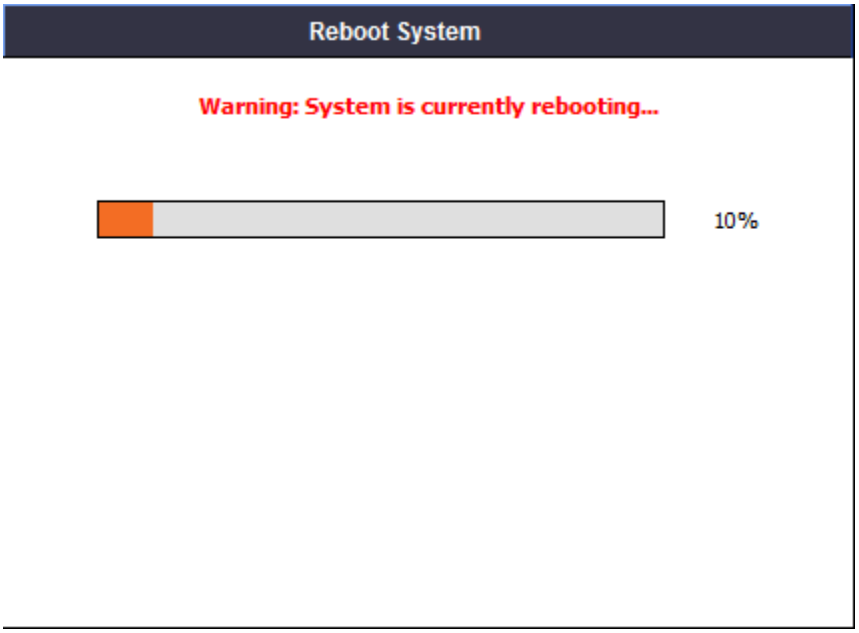

Reboot System
Do you want to save the settings ?
Yes
No
Reboot
If you do not save the settings, all changes made in this session will be lost.

Selecting the **Yes** radio button will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Selecting the **No** radio button instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the **Reboot** button to restart the Switch.

Figure 317: System Rebooting window



A System Log Entries

APPENDIX

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity	Remark
System	System started up	System started up	Critical	
	System warm start	System warm start	Critical	
	System cold start	System cold start	Critical	
	Configuration saved to flash	Configuration saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	System log saved to flash	System log saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration and log saved to flash	Configuration and log saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Internal Power failed	Internal Power failed	Critical	

Category	Event Description	Log Information	Severity	Remark
	Internal Power is recovered	Internal Power is recovered	Critical	
	Redundant Power failed	Redundant Power failed	Critical	
	Redundant Power is working	Redundant Power is working	Critical	
	Side Fan failed	Side Fan failed	Critical	
	Side Fan recovered	Side Fan recovered	Critical	
Up/Download	Firmware upgraded successfully	Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Firmware upgrade was unsuccessful	Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration successfully downloaded	Configuration successfully downloaded by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.

Category	Event Description	Log Information	Severity	Remark
	Configuration successfully uploaded	Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration upload was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Log message successfully uploaded	Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Log message upload was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Firmware successfully uploaded	Firmware successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.

Category	Event Description	Log Information	Severity	Remark
	Firmware upload was unsuccessful	Firmware upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
Interface	Port link up	Port <portNum> link up, <link state>	Informational	link state, for ex: , 100Mbps FULL duplex
	Port link down	Port <portNum> link down	Informational	
Console	Successful login through Console	Successful login through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console	Login failed through Console (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Logout through Console	Logout through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Console session timed out	Console session timed out (Username: <username>)	Informational	There are no IP and MAC if login by console.
Web	Successful login through Web	Successful login through Web (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>)	Informational	
	Web session timed out	Web session timed out (Username: <username>, IP: <ipaddr>)	Informational	
	Successful login through Web(SSL)	Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Web(SSL)	Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Web(SSL)	Logout through Web(SSL) (Username: <username>, IP: <ipaddr>)	Informational	
	Web(SSL) session timed out	Web(SSL) session timed out (Username: <username>, IP: <ipaddr>)	Informational	

Category	Event Description	Log Information	Severity	Remark
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>)	Informational	
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>)	Informational	
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational	
STP	Topology changed	Topology changed (Instance:<InstanceID> ,Port:<portNum>,MAC:<macaddr>)	Informational	
	New Root selected	[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>)	Informational	
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational	
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational	
	New root port	New root port selected (Instance:<InstanceID>, port:<portNum>)	Notice	
	Spanning Tree port status changed	Spanning Tree port status change (Instance:<InstanceID> , Port:<portNum>) <old_status> -> <new_status>	Notice	
	Spanning Tree port role changed	Spanning Tree port role change (Instance:<InstanceID> , Port:<portNum>) <old_role> -> <new_role>	Informational	
	Spannnig Tree instance created	Spanning Tree instance created (Instance:<InstanceID>)	Informational	
	Spannnig Tree instance deleted	Spanning Tree instance deleted (Instance:<InstanceID>)	Informational	
	Spanning Tree Version changed	Spanning Tree version change (new version:<new_version>)	Informational	
	Spanning Tree MST configuration ID name and revision level changed	Spanning Tree MST configuration ID name and revision level change (name:<name> ,revision level <revision_level>).	Informational	

Category	Event Description	Log Information	Severity	Remark
	Spanning Tree MST configuration ID VLAN mapping table deleted	Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [-<endvlanid>])	Informational	
	Spanning Tree MST configuration ID VLAN mapping table added	Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [-<endvlanid>])	Informational	
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>,)	Warning	
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational	
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational	
	SSH server is enabled	SSH server is enabled	Informational	
	SSH server is disabled	SSH server is disabled	Informational	
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational	
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational	
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Web authenticated by AAA local method	Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web(SSL) authenticated by AAA local method	Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Informational	

Category	Event Description	Log Information	Severity	Remark
	Login failed through Web(SSL) authenticated by AAA local method	Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>,)	Informational	
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web(SSL) authenticated by AAA none method	Successful login through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	

Category	Event Description	Log Information	Severity	Remark
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Web(SSL) authenticated by AAA server	Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Web(SSL) authenticated by AAA server	Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web(SSL) due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Telnet due to AAA server timeout or improper configuration	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through SSH authenticated by AAA server	Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through SSH due to AAA server timeout or improper configuration	Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	

Category	Event Description	Log Information	Severity	Remark
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>,)	Informational	
	Enable Admin failed through Web(SSL) authenticated by AAA local_enable method	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Telnet authenticated by AAA local_enable method	Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through <Telnet or Web or SSH> from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational	

Category	Event Description	Log Information	Severity	Remark
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Web(SSL) authenticated by AAA none method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web due to AAA server timeout or improper configuration	Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA server	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	

Category	Event Description	Log Information	Severity	Remark
	Enable Admin failed through Web(SSL) authenticated by AAA server	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
Port Security	port security is exceeded to its maximum learning size and will not learn any new address	Port security violation (MAC address: <macaddr> on port: <portNum>)	Warning	
MBAC	A host fails to pass the authentication	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <portNum>, VID: <vid>)	Critical	
	The authorized user number on a port reaches the max user limit.	Port <portNum> enters MAC-based Access Control stop learning state.	Warning	per port
	The authorized user number on a port is below the max user limit in a time interval(interval is project depended).	Port <portNum> recovers from MAC-based Access Control stop learning state.	Warning	per port

Category	Event Description	Log Information	Severity	Remark
	The authorized user number on whole device reaches the max user limit.	MAC-based Access Control enters stop learning state.	Warning	per system
	The authorized user number on whole device is below the max user limit in a time interval(interval is project depended).	MAC-based Access Control recovers from stop learning state.	Warning	per system
	A host passes the authentication	MAC-based Access Control host login successful (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational	
	A host is aged out	MAC-based Access Control host aged out (MAC: <macaddr>, port: <portNum>, VID: <vid>)	Informational	
WAC	A user fails to pass the authentication	WAC unauthenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Warning	
	A user passes the authentication	WAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Warning	
	The authorized user number on whole device reaches the max user limit.	WAC enters stop learning state.	Warning	per system
	The authorized user number on whole device is below the max user limit in a time interval(interval is project depended).	WAC recovers from stop learning state.	Warning	per system
IP and Password Changed	IP Address change activity	Management IP address was changed by console(Username: <username>,IP:<ipaddr>)	Informational	"console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Password change activity	Password was changed by console (Username: <username>,IP:<ipaddr>)	Informational	"console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
Loop Back Detection	Port loop occurred	Port <portNum> LBD loop occurred. Port blocked	Critical	
	Port loop detection restarted after interval time	Port <portNum> LBD port recovered. Loop detection restarted	Informational	

Category	Event Description	Log Information	Severity	Remark
Gratuitous ARP	Gratuitous ARP detected duplicate IP.	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>, Interface: <ipif_name>).	Warning	
BPDU Protection	BPDU attack happened	Port <portNum> enter BPDU under attacking state (mode: drop / block / shutdown)	Informational	
	BPDU attack automatically recover	Port <portNum> recover from BPDU under attacking state automatically	Informational	
	BPDU attack manually recover	Port <portNum> recover from BPDU under attacking state manually	Informational	
Monitor	Temperature exceeds confidence level	Temperature Sensor <sensorID> enter alarm state. (current temperature: <temperature>)	Warning	
	Temperature recovers to normal.	Temperature Sensor <sensorID> recovers to normal state. (current temperature: <temperature>)	Informational	
CFM	Cross-connect is detected	CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Critical	
	Error CFM CCM packet is detected	CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Warning	
	Can not receive remote MEP's CCM packet	CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Warning	
	Remote MEP's MAC reports an error status	CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Warning	
	Remote MEP detects CFM defects	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>)	Informational	
CFM Extension	AIS condition detected	AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	

Category	Event Description	Log Information	Severity	Remark
	AIS condition cleared	AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
	LCK condition detected	LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
	LCK condition cleared	LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
Voice VLAN	When a new voice device is detected in the port	New voice device detected (MAC:<macaddr>,Port:<portNum>)	Informational	
	While the port join to the voice VLAN while the port is auto voice VLAN mode	Port <portNum> add into voice VLAN <vid >	Informational	
	While the port withdraws from the voice VLAN while there is no more voice device detected in the aging interval.	Port <portNum> remove from voice VLAN <vid >	Informational	
Command Logging	Command Logging	<username>: execute command "<string>".	Informational	

APPENDIX B

Trap Log Entries

This table lists the trap logs found on the Switch.

Trap Name	Trap Description	OID
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.3
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.4
authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmRisingThreshold	1.3.6.1.2.1.16.0.1

Trap Name	Trap Description	OID
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmFallingThreshold	1.3.6.1.2.1.16.0.2